ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

Борьба с киберпреступностью в условиях развития цифрового общества

Сборник научных статей Международной конференции «Борьба с киберпреступностью в условиях развития цифрового общества»

Московский университет МВД России
имени В.Я. Кикотя, 2019

ISBN 978-5-9694-0824-1

Москва
2019

ББК 67.408.1
Б84

Рецензенты:
старший преподаватель кафедры информационной безопасности Воронежского института МВД России кандидат технических наук **Зарубин С. В.**; профессор кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор **А. В. Еськов**

Б84 **Борьба с киберпреступностью в условиях развития цифрового общества** : сборник научных статей Международной конференции «Борьба с киберпреступностью в условиях развития цифрового общества» 2019 г. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 200 с. − 1 электронный оптический диск (CD-R). − Системные требования : CUP 1,5 ГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске
ISBN 978-5-9654-0824-1

Всероссийская конференция «Борьба с киберпреступностью в условиях развития цифрового общества» посвящена проблемам раскрытия и расследования преступлений в сфере компьютерной информации, а также практическим аспектам обеспечения информационной безопасности компьютерных сетей.

Эффективная борьба с киберпреступностью предполагает своевременное реагирование и всестороннее изучение специфики преступлений, заключающейся в пересечении юридических и технических научных знаний.

В сборник вошли статьи преподавателей, курсантов, слушателей и практических работников, специализирующихся на раскрытии и расследовании преступлений в сфере компьютерной информации. Отражены проблемные вопросы и перспективные направления по борьбе с киберпреступностью в условиях цифровизации общества.

ББК 67.408.1

ISBN 978-5-9654-0824-1

Научное электронное издание

Корректор *Чеботарева С. О.*
Компьютерная верстка *Фомин И. Е.*
11,52 усл. печ. л.
Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http: //www.mosu.mvd.ru, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Боровиков Валерий Борисович[1]*,*
профессор кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент,
заслуженный сотрудник ОВД России

Боровикова Виктория Валерьевна[2]*,*
доцент кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ВОПРОСЫ НАКАЗАНИЯ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Наказание за совершение преступлений в сфере компьютерной информации (гл. 28 УК РФ) преследует те же цели, что и за другие преступления: восстановление социальной справедливости, исправление осужденного и предупреждение совершения новых преступлений (ч. 2 ст. 43 УК РФ). Вместе с тем надо помнить, что цель общей превенции (общего предупреждения) имеет здесь большее значение, чем в отношении иных преступлений, поскольку среди значительного числа пользователей информационными технологиями (среди них немало несовершеннолетних) деяния, запрещенные ст.ст. 272–274.1 УК РФ, не воспринимаются как что-то вредоносное, возмутительное, не соответствующее социальным установкам личности. В таких ситуациях цель достижения исправления осужденных достаточно затруднительна, ибо требует коренной перемены ценностных ориентаций в основном молодого поколения людей, для которых использование информационных технологий даже в преступных целях является своеобразным способом самоутверждения в своей среде, источником решения жизненных проблем, в том числе материального характера.

Примерно те же соображения определяют специфику целей восстановления социальной справедливости в отношении лиц, совершивших преступления в сфере компьютерной информации. Как известно, принцип социальной справедливости выражается в том, что наказание и иные меры уголовно-правового характера, применяемые к лицу, совершившему преступление, должны соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения и личности виновного (ст. 6 УК РФ). Но общественное мнение, повлиявшее и на законодателя при выборе им санкций за данные деяния, еще не сформировалось в полной мере у нас в стране по поводу степени репрессивности, которую должны содержать те или иные виды уголовных наказаний за рассматриваемые преступления. Поэтому цели специального и общего предупреждения, на наш взгляд, преобладают над другими целями наказания в отношении лиц, совершивших преступление в сфере компьютерной информации.

Под этим углом зрения надо, прежде всего, и оценивать нынешние санкции, содержащиеся в уголовно-правовых нормах, регламентирующих ответственность за анализируемые преступления.

Прежде всего при изучении содержания ст.ст. 272–274.1 УК РФ обращает на себя внимание то, что ни одно из преступлений в сфере компьютерной информации не относится к категории особо тяжких. Тяжкими преступлениями признаются деяния, предусмотренные ч. 4 ст. 272, ч. 3 ст. 273, ч. 2–5 ст. 274.1 УК РФ. Естественно, и наказания за их совершение не выглядят достаточно суровыми. Наиболее строго наказывается неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, если оно повлекло тяжкие последствия (ч. 5 ст. 274.1 УК РФ), влекущее за собой лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Другие преступления рассматриваемой группы наказываются значительно менее строго. Так, за неправомерный доступ к компьютерной информации без отягчающих обстоятельств (ч. 1 ст. 272 УК РФ) наиболее жестким выглядит наказание в виде лишения свободы на срок до 2 лет. Аналогично наказывается нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей без отягчающих обстоятельств (ч. 1 ст. 274 УК РФ).

Деяния, предусмотренные чч. 2–3 ст. 272 УК РФ (Неправомерный доступ к компьютерной информации), чч. 1–2 ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ), ч. 2 ст. 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей при отягчающих обстоятельствах), ч. 1 ст. 274.1 УК РФ (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации), относятся к категории средней тяжести (максимальное наказание в настоящее время за умышленные деяния до 5 лет лишения свободы).

Причем в девяти нормах (чч. 1–4 ст. 272, чч. 1–3 ст. 273, чч. 1–2 ст. 274 УК РФ) законодатель использует в отношении наказания в виде лишения свободы формулировку без указания на его минимальные пределы. Получается, что в соответствии с ч. 2 ст. 56 УК РФ оно может составить 2 месяца лишения свободы, что также свидетельствует о недостаточно внимательном подходе законодателя к конструированию санкций уголовно-правовых норм, предусматривающих ответственность за преступления в сфере компьютерной информации. Вряд ли такие краткие сроки лишения свободы имеют в подобных случаях эффективность.

Нужны уточнения на законодательном уровне санкций уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации. Общественная опасность данных преступлений будет только расти и уже сейчас они причиняют огромный вред[1].

---

[1] Подробнее об этом, см., например: Жестеров П. В. Концепция уголовной репрессии в формирующемся цифровом обществе // Уголовное право: стратегия развития в XXI веке : материалы XVI международной научно-практической конференции. М. : РГ-Пресс, 2019. С. 44–47 ; Ларина Е., Овчинский В. Новизна // Завтра. – 2017. – № 11, 12, 14 ; Гончаров А. Битва за Рунет // Завтра. – 2019. – № 43.

По нашему мнению, в принципе эти преступления должны признаваться без отягчающих обстоятельств преступлениями средней тяжести (за исключением деяния, предусмотренного ст. 274.1 УК РФ). Причем минимальное наказание в виде лишения свободы должно составлять не менее 6 месяцев (это минимальный период времени, когда возможно, как показывает уголовно-исполнительная практика, организовать процесс исправления осужденного к лишению свободы). При наличии отягчающих обстоятельств (крупного ущерба, наличия корыстной заинтересованности, использования лицом своего служебного положения, группы лиц по предварительному сговору, организованной группы) деяния, предусмотренные ст.ст. 272–274 УК РФ, должны признаваться тяжкими преступлениями. Соответственно, и санкции за совершение этих деяний должны содержать более строгие наказания. Напомним, что в связи с изменениями, которые имели место после принятия Федерального Закона Российской Федерации от 17 июня 2019 г. № 146-ФЗ, неосторожные преступления средней тяжести могут наказываться на срок, не превышающий 10 лет лишения свободы, а тяжкие неосторожные преступления – на срок, не превышающий 15 лет лишения свободы (это положение в законе может быть учтено, например, при конструировании санкций, предусмотренных ч. 2 ст. 274, ч. 3 ст. 274.1 УК РФ).

Еще более жесткие санкции должны быть предусмотрены за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Даже без отягчающих обстоятельств указанное преступление (ч. 1 ст. 274.1 УК РФ) целесообразно признавать тяжким преступлением, а не преступлением средней тяжести, как это имеет место сейчас. Следовательно, и наказание за его совершение должно превышать 5 лет лишения свободы.

Разумеется, есть смысл с учетом повышенной общественной опасности данных деяний, содержащих квалифицированные составы повысить размеры этих санкций. Это необходимо сделать в интересах общей превенции (о чем шла речь в начале нашей статьи).

Наконец, при наличии признаков особо квалифицированного состава неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, повлекшего тяжкие последствия, есть смысл признавать это деяние особо тяжким (т. е. наказание должно превышать 10 лет лишения свободы).

Проблема совершенствования санкций уголовно-правовых норм, содержащихся в ст.ст. 272–274.1 УК РФ, во многом связана с тем, что законодатель для описания содеянного использует оценочные признаки составов преступлений. Так, в чч. 2–3 ст. 274.1 УК РФ в качестве необходимого условия наступления уголовной ответственности законодатель называет причинение вреда критической информационной инфраструктуре Российской Федерации.

В ч. 4 ст. 272, ч. 3 ст. 273 и ч. 2 ст. 274 УК РФ квалифицирующим признаком, т. е. повышающим уголовную ответственность, признается наступление тяжких последствий или угрозы их наступления.

В ч. 5 ст. 274.1 УК РФ предусмотрена ответственность за деяния, указанные в чч. 1–4 этой статьи, если они повлекли тяжкие последствия.

Возникают закономерные вопросы. Что следует понимать под причинением вреда критической информационной инфраструктуры Российской Федерации? Какой смысл вкладывает законодатель в понятие тяжких последствий или угрозы их наступления[1]. Ни в законе, ни на уровне постановления Пленума Верховного Суда Российской Федерации ответов нет. Конечно, это недопустимо, так как не зная содержания названных выше признаков составов преступлений, трудно дать правильную оценку содеянного и в конечном итоге назначить справедливое обоснованное наказание лицам, признанным виновными в его совершении.

Нужны соответствующие разъяснения. В идеале в самом законе должны содержаться положения на этот счет. Если это не произойдет, то такие рекомендации должен дать Пленум Верховного Суда Российской Федерации в специально принятом постановлении, посвященном применению уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации (потребность в принятии подобного документа давно созрела).

Возможен вариант с включением соответствующего пункта по данным вопросам в какое-либо уже из действующих постановлений Пленума Верховного Суда Российской Федерации, например, от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (данный вариант решения возникшей ситуации рекомендуется только в связи с отсутствием специального постановления, посвященного вопросам ответственности за анализируемые преступления).

В частности, заслуживает внимания п. 8 этого постановления, в котором дается понятие «иных тяжких последствий» применительно к п. «в» ч. 2 ст. 205 УК РФ. К разновидностям таких последствий Пленум Верховного Суда Российской Федерации относит, например, дезорганизацию деятельности органов государственной власти и местного самоуправления; длительное нарушение работы предприятия (предприятий) и (или) учреждения (учреждений), существенное ухудшение экологической обстановки и т. д.

В любом случае подобные разъяснения способствовали бы единообразию в определении этих последствий, правильной квалификации содеянного и назначению наказания за указанные выше деяния.

[1] См. подробнее позиции по этому вопросу, например: Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е. А. Русскевич. М. : Инфра-М, 2019. С. 115–116.

Лукьянов Александр Сергеевич[1]**,**
старший преподаватель кафедры инфокоммуникационных систем и технологий
Воронежского института МВД России

Гилев Игорь Владимирович[2]**,**
адъюнкт кафедры инфокоммуникационных систем и технологий
Воронежского института МВД России

Попов Алексей Вячеславович[3]**,**
курсант 4 курса радиотехнического факультета
Воронежского института МВД России

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ СВЯЗИ И КОМПЬЮТЕРНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ОРТОГОНАЛЬНЫХ ВЕЙВЛЕТ-ФУНКЦИЙ

Задача повышения надежности функционирования компьютерных сетей и помехоустойчивости сигналов, передаваемых по каналам специальной связи, имеет первостепенное значение для органов внутренних дел. Нарушение целостности, конфиденциальности и доступности информации такого уровня может привести к нежелательным последствиям и нанести ущерб функционированию подразделений. Качество связи характеризуется отношением сигнал/шум, поэтому при наложении на спектр сигнала аддитивной помехи необходимой мощности и полосы пропускания детектирование сигнала на приемной стороне станет невозможным, либо будет сопровождаться большим количеством ошибок. На данный момент существует довольно много способов защиты сигналов от непреднамеренных и преднамеренных помех. Основными из них являются:

- использование адаптивных систем радиосвязи;
- применение помехоустойчивого кодирования;
- повышение выходной мощности сигнала, тем самым увеличение отношения сигнал/шум;
- рациональный выбор модуляции сигналов.

Рассмотрим широкополосные сигналы, которые благодаря расширенному спектру обладают меньшей интенсивностью и сложнее поддаются обнаружению, поскольку анализаторы спектра не могут с требуемой точностью идентифицировать наличие сигнала в канале связи. Для расширения спектра сигнала используются определенные виды модуляции (к примеру, частотная или фазовая), либо адаптивные системы радиосвязи, в которых несущая частота сигнала генерируется случайным образом псевдослучайной последовательностью (ПСП). Если для генерации ПСП используются биортогональные вейвлет-функции, спектр можно расширить в 3–3,5 раза относительно фазовой модуляции [1].

Вейвлет-преобразование является математическим инструментом для иерархической декомпозиции функции, представляется в виде обобщенного ряда Фурье по системе базисных функций, которые локализуются как во временной, так и в частотной областях [2]. Оно несет большое количество информации о сигнале, с его помощью может производиться низкочастотная аппроксимация спектра сигнала. Поэтому, если имеются сведения о вейвлет-преобразовании на передающей стороне, то передаваемый сигнал можно восстановить с необходимой точностью, даже несмотря на то, что информация о сигнале содержится в сравнительно небольшом наборе значений. К вейвлет-функциям (вейвлетам) применима операция масштабирования, что позволяет детализировать объекты передачи, независимо от их формата (изображения, видео-, аудиофайлы и т. д.). При масштабе вейвлета в некоторое число раз и смещении его во времени на фиксированное расстояние, которое зависит от масштаба, все сдвиги будут являться попарно ортогональными – такое преобразование будет называться «ортогональным».

Вейвлет-функцию для аналоговых сигналов можно представить, как:

$$\psi_{ab}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right), \text{ где} \quad (1)$$

a – масштаб базисной функции, b – временной сдвиг.

В дискретном виде параметр масштаба $a = 2^p$, где p – любое целое положительное число; временной сдвиг $b = k \cdot 2^p$.

В результате преобразований функция принимает вид:

$$\psi_{pk}(t) = \frac{1}{\sqrt{2^p}}\psi(2^{-p} \cdot t - k). \quad (2)$$

Указанный алгоритм [3] позволяет графически представить вейвлет-функции в частотной и временной областях. Реализация данного алгоритма представлена ниже (*рис. 1–3*).

Как видно из *рис. 3*, управлять шириной спектра вейвлет-функции можно за счет изменения масштаба базисной функции a. Поэтому в системе радиосвязи либо компьютерной сети помимо блока генератора псевдослучайной последовательности подключается устройство, генерирующее вейвлет ($\psi_{ab}(\omega)$ при $a \to 0$). На *рис. 4* представлена часть структурной схемы передающего устройства адаптивной системы с подключением вейвлет-функции.

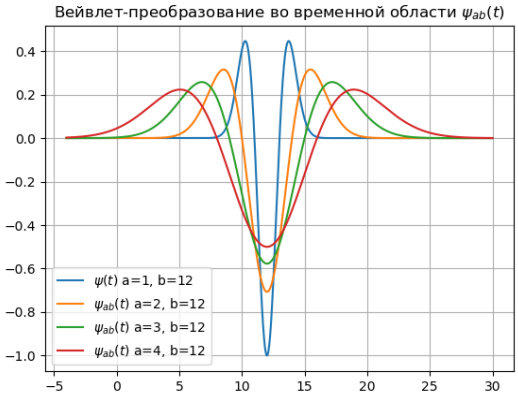

Рис. 1. Вейвлет-функция $\psi_{ab}(t)$ при изменении параметра a

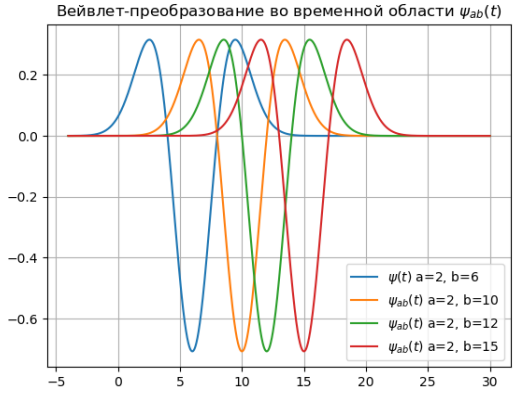

Рис. 2. Вейвлет-функция $\psi_{ab}(t)$ при изменении параметра b

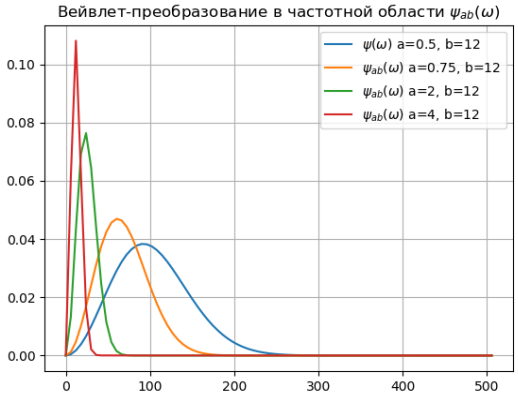

Рис. 3. Вейвлет-функция $\psi_{ab}(\omega)$ при изменении параметра a

Если в исходной структурной схеме сигнал на кодер, фазовый модулятор и генератор вспомогательной последовательности поступал с генератора псевдослучайной последовательности, то в данной схеме сигнал поступает с перемножителя, реализующего наложение вейвлет-функции на генератор псевдослучайной последовательности.

Рис. 4. Часть структурной схемы передатчика адаптивной системы с подключением вейвлет-функции

Функционирование компьютерных сетей оптимизируется в первую очередь благодаря тому, что коэффициенты вейвлет-функции содержат практически всю

информацию об анализируемом процессе. В зависимости от типа передаваемой информации коэффициенты вейвлета могут изменяться как пользователем, так и автоматически при установке соответствующих настроек сети. Используя разные коэффициенты, можно выявить те или иные свойства исследуемого процесса в компьютерной сети и системе радиосвязи[1].

Таким образом, использование вейвлет-функций является актуальным методом повышения эффективности функционирования таких сетей и систем, где прежде широко применялись иные методы анализа и представления данных (к примеру, преобразование Фурье). Высокая эффективность алгоритмов, применение в частотно-временной области и устойчивость к воздействию помех делает вейвлет-функцию мощным инструментом в области анализа и передачи информационного ресурса.

Список литературы

1. Никитин М. Л. Способы повышения помехоустойчивости широкополосных сигналов / М. Л. Никитин, А. Н. Копысов, В. В. Хворенков // Радиотехника, электроника и связь (РЭИС-2015) : сборник материалов III Международной научно-технической конференции. – Омский научно-исследовательский институт, 2017. – С. 375–378.

2. Вейвлет-анализ [Электронный ресурс] // URL: http://wiki.technicalvision.ru/index.php/Вейвлет-анализ (дата обращения: 05.11.2019).

3. Вейвлет-анализ. Основы [Электронный ресурс] // URL: https://habr.com/ru/post/449646 (дата обращения: 05.11.2019).

4. Хохлов Н. С. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты / Н. С. Хохлов [и др.] // Вестник Поволжского государственного технологического университета. – Серия: Радиотехнические и инфокоммуникационные системы. – 2019. – № 1. – С. 22–30.

[1] Варламова М. А. Применение вейвлет-преобразований в системах локализации черт лица человека / М. А. Варламова [Электронный ресурс] // URL: https://docplayer.ru/76120131-Primenenie-veyvlet-preobrazovaniy-v-sistemah-lokalizacii-chert-lica-cheloveka.html (дата обращения: 07.11.2019).

Виноградова Ольга Павловна[1]*,*
доцент кафедры криминалистики
Уральского юридического института МВД России,
кандидат юридических наук

Дерюгин Роман Александрович[2]*,*
старший преподаватель кафедры криминалистики
Уральского юридического института МВД России,
кандидат юридических наук

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РЕАЛИЯХ СОВРЕМЕННОЙ РОССИИ И ПУТИ ИХ РЕШЕНИЯ

На протяжении многих лет люди пытаются улучшить качество своей жизни, усовершенствовав имеющиеся технологии. Сложно представить жизнедеятельность современного человека, не использующего достижения научного и технического прогресса, так в нашей повседневной жизни появились компьютер и сеть Интернет, сотовая связь и мобильный телефон и т. п. Всеобщая компьютеризация и информатизация населения позволяют намного быстрее и качественнее решать повседневные задачи и достигать определенных целей.

К сожалению, все активнее технические новшества используются преступниками, что подтверждается официальной статистикой. Так, за январь – сентябрь 2019 г. с использованием компьютерных и информационно-телекоммуникационных технологий было совершено 156 307 преступлений, а за аналогичный период предыдущего года – 82 440 [1]. Кроме того, возросло число преступлений в сфере информационно-телекоммуникационных технологий. По данным Генеральной прокуратуры Российской Федерации в 2018 г. их количество увеличилось с 65 949 до 90 587. Доля таких преступлений от числа всех зарегистрированных в России преступных деяний составляет 4,4 % – фактически это каждое двадцатое преступление [2]. Показатели первого полугодия 2019 г. также свидетельствуют о росте указанной категории преступлений (+3,4 %).

Анализируя судебную и следственную практику, можно сделать вывод о том, что самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). В то время как раскрываемость преступлений в сфере информационно-телекоммуникационных технологий ежегодно колеблется от 45 до 53 % [1].

Полагаем, что проблема противодействия киберпреступности остается крайне актуальной, требующей особо пристального внимания со стороны правоохранительных органов и государства. Действительно, развитие информационно-телекоммуникационных и компьютерных технологий, сопровождается

активной деятельностью преступников. Однако проблема заключается не только в увеличении числа киберпреступлений, но и в повсеместном распространении таких преступлений во всех сферах. Новейшие компьютерные и информационные технологии используются при незаконном обороте наркотических средств и психотропных веществ, пропаганде деструктивной идеологии, при совершении различного рода мошеннических действий, незаконных финансовых операций и других преступлений.

Проанализировав современное состояние информационно-телекоммуникационного пространства и аналитических сведений о состоянии преступности и технической оснащенности правоохранительных органов, можно выделить ряд проблем, требующих скорейшего решения:

– отсутствует эффективное взаимодействие органов внутренних дел с государством, обществом и учреждениями в сфере кибербезопасности, а меры по противодействию киберугрозам остаются на декларативном уровне. Например, до настоящего времени не сформирована система оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и даже с операторами сотовой связи, что влияет на раскрытие преступлений «по горячим следам», позволяя преступниками тщательно скрыть следы противоправных действий, не до конца урегулирована система государственных учреждений, проводящих компьютерно-технические и иные судебные экспертизы по делам о таких преступлениях;

– деятельность по раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных и компьютерных технологий основана на методах, некоторые из которых уже неэффективны. Современные правоохранительные органы с имеющимся арсеналом технических средств и технологий не всегда могут противопоставить себя «новой киберпреступности»;

– не сформированы предмет, методы, цели и задачи цифровой криминалистики. Это новое перспективное направление, требующее осмысления и научного развития ввиду необходимости разработки практических рекомендаций по работе с электронными (виртуальными) цифровыми следами, с компьютерной техникой, с интернет-сервисами, приложениями и программным обеспечением. Современный правоохранитель обязан владеть такими навыками;

– недостаточно эффективна система подготовки юридических и технических кадров. В вузах, осуществляющих подготовку сотрудников органов внутренних дел. необходимо разрабатывать новые спецкурсы, посвященные расследованию преступлений в сфере информационно-телекоммуникационных технологий и информационной безопасности. В качестве общей проблемы повсеместно отмечается невысокий уровень компьютерной грамотности и осведомленности о современных киберугрозах большинства населения, в том числе государственных служащих [3].

– недостаточно совершенно законодательство в области противодействия киберпреступлениям (например, не установлена уголовная ответственность за компьютерные преступления, основанные на принципах социального инжиниринга, и рассылку вредоносного спама как отдельный вид преступлений) [4].

На наш взгляд, проведенный анализ содержит далеко не все проблемы, связанные с кибербезопасностью общества и государства. Более того, с развитием информационно-телекоммуникационных технологий будут появляться новые способы совершения преступлений и методы противодействия правоохранительным органам.

Современные условия жизни заставляют бороться с анонимными и неконтролируемыми сервисами, использованием приложений-мессенджеров в преступных целях, «серыми» SIM-картами. Безусловно, нельзя просто ограничить доступ к тем или иным интернет сервисам. Без должного правового регулирования указанную проблему решить невозможно, необходимо повышать ответственность за размещение в сети запрещенного контента, формировать правовые и организационно-технические механизмы регулирования на противоправную деятельность в данной сфере.

Очевидно, что государство ведет активную политику в рамках противодействия киберпреступности и преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Однако в данный момент эти меры не профилактические, а, по большей части, контрмеры против уже совершенных противоправных действий.

Список литературы

1. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс] // URL: http://mvd.ru/presscenter/statistics/reports/item/804701 (дата обращения: 11.11.2019).

2. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс] // URL: https://genproc.gov.ru/smi/news/news-1431104 (дата обращения: 12.11.2019).

3. Латышов И. В. Проблемы совершенствования учебно-материальной базы образовательных организаций системы МВД России при подготовке экспертов-криминалистов // Вестник Московского университета МВД России. – № 1. – 2018. – С. 193–197.

4. Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемых с использованием информационных технологий : сборник статей Международной научно-практической конференции: Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). – М. : Академия управления МВД России, 2018. – С. 75.

Зайцев Петр Викторович[1]**,**
старший оперуполномоченный
ООРИ ГУ МВД России по Красноярскому краю

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СИСТЕМ БИОМЕТРИЧЕСКОГО РАСПОЗНАВАНИЯ ЧЕЛОВЕЧЕСКОГО ЛИЦА НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И НЕЙРОННЫХ СЕТЕЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Двадцать первый век можно назвать веком искусственного интеллекта, развитие которого определяет дальнейшее будущее человечества. На сегодняшний день искусственный интеллект применяется в различных областях человеческой деятельности – от медицины до систем управления космическими аппаратами. В целях совершенствования работы по развитию данного направления в России 10 октября 2019 г. Президентом Российской Федерации был подписан Указ «О развитии искусственного интеллекта в Российской Федерации» [4].

Одним из направлений развития искусственного интеллекта являются нейронные сети, представляющие собой математическую модель и ее программно-аппаратную реализацию, построенную по принципу организации биологических нейронных сетей живого мозга.

Учитывая, что одним из приоритетных направлений деятельности правоохранительных органов России является применение новых технологий различных отраслей наук в раскрытии и профилактике преступлений, становится актуальной тема применения искусственного интеллекта и нейронных сетей в решении задач, стоящих перед органами внутренних дел Российской Федерации.

В данной статье рассматриваются имеющийся в подразделениях ОВД опыт применения нейронных сетей для решения задач, связанных с биометрической идентификацией человеческих лиц, проблемы, возникающие в данном направлении, предлагаемые подходы и конкретные функциональные решения, предлагается оценить перспективы развития и применения информационных систем, основанных на искусственном интеллекте.

На сегодняшний день одним из наиболее востребованных и перспективных направлений применения искусственных нейронных сетей в деятельности ОВД являются системы биометрической идентификации лица по его изображению. Ниже рассмотрены практические возможности их применения:

– оперативные опознание и идентификация лиц, совершивших преступление или подозреваемых в их совершении, лиц пропавших без вести по базе фотоизображений, которые формируются в результате внутри- и межведомственного взаимодействия – ФМС России, ГИБДД России, ФСИН России, фотографии лиц, доставленных в отделы полиции за совершение правонарушений и другие источники;

---

[1]

– построение аналитических систем, позволяющих выявлять принадлежность лиц к конкретным социальным группам и организациям, используя в виде источника для анализа фото- и видеоматериалы, находящиеся в свободном доступе в сети Интернет, в том числе в социальных сетях;

– обеспечение безопасности на массовых мероприятиях и в местах большого скопления людей, выявление на рубежах контроля лиц, стоящих на оперативных учетах, а также находящихся в розыске.

Из наиболее часто применяемых в ОВД систем биометрической идентификации лиц по фотоизображениям можно выделить – АИПС «Сова», АИПС «Портрет-поиск», СПО АИС «Синергет-розыск». Опыт работы с данными системами выявляет ряд проблем и недостатков:

– необходимость участия оператора при кодировании изображения;
– низкое качество идентификации;
– отсутствие возможности распознавания лиц на групповых фотографиях;
– невозможность работы с видеопотоком;
– высокие требования к условиям расположения лица на фотоизображении;
– высокая стоимость лицензии.

В настоящее время сообществом разработчиков свободного программного обеспечения предоставлено множество библиотек на полной Open Source лицензии, реализующих алгоритмы сверточных нейронных сетей, обученных HOG-каскадов для поиска лиц, подборки функций матричной геометрии и методы для преобразования графических изображений. В пример можно привести проекты библиотек с открытым исходным кодом *dLib* [5] и *openCV* [6].

На базе функционала данных библиотек и моделей уже обученных нейронных сетей, находящихся в свободном доступе (“*shape predictor 68 face landmarks*”, “*face_recognition*”, “*mmod_human_face_detector*”) представляется возможной реализация систем биометрической идентификации, отвечающих современным требованиям. Такой разработкой в настоящее время занимаются сотрудники программно-технического отделения ООРИ ГУ МВД по Красноярскому краю. Накоплен практический опыт применения моделей сверточных нейронных сетей в разработке автоматизированных информационно-поисковых систем. Ниже будет представлено схематичное описание пилотного проекта *FaceID*, представляющего собой программный комплекс биометрической идентификации и поиска лиц (*рис. 1*).

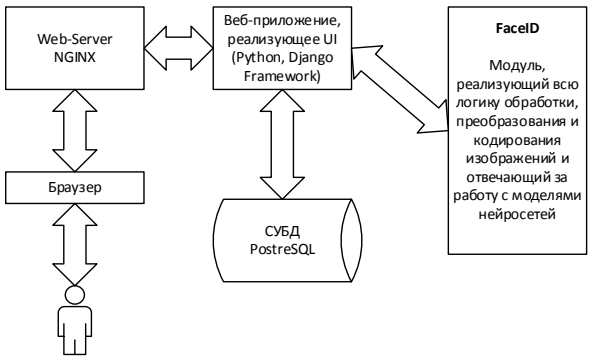

Рис. 1. Блок-схема проекта

Рассмотрим общий алгоритм работы модуля биометрического распознавания лиц *FaceID*, основные применяемые в нем библиотеки и модели нейросетей. Механизм получения, преобразования и ввода данных:

– библиотека *imUtils* – преобразование размера исходного изображения;

– применения алгоритма модели нейронной сети *mmod human face detector*, обученной на выявление человеческих лиц на фотографии;

– использование библиотеки *dLib* и модели нейронной сети *shape predictor 68 face landmarks* для получения геометрических моделей найденных на фотоизображении лиц, представленных в виде набора точек, описывающих положение частей лица на плоскости;

– выравнивание вырезанных из исходной фотографии лиц по ранее полученным точкам расположения глаз и путем подсчета угла наклона лица на изображении;

– использование библиотеки *openCV* и модели сверточной нейронной сети *face recognition CNN* для построения *dataset*'а, описывающего геометрические модели ранее найденных на фотографии лиц и их сохранение в сегменте нейросети.

Процесс поиска похожих лиц осуществляется по следующему алгоритму:

– модулю *FaceID* передается исходное фотоизображение;

– производятся те же действия по обнаружению, преобразованию и кодированию лиц, что и при вводе данных, описанном выше;

– сравнение векторов кодированной биометрической модели исходного лица с векторами моделей, занесенных в текущий сегмент нейросети и вычисление коэффициента кореляции, который и определяет сходство исходного лица с лицами, модели которых хранятся в сегменте нейросети.

Тестирование системы на «учебном» массиве данных показывает достойные результаты как по скорости, так и по качеству поиска лиц. Таким образом, на поиск лица в сегменте нейросети из ста тысяч кодированных моделей требуется около 1–2 с.

Можно выделить существенные преимущества подхода применения проектов с открытым исходным кодом на основе искусственных нейронных сетей:

– значительная экономия бюджетных средств за счет использования разработок на *open source* лицензии;

– гибкость и возможность настройки продукта под текущие задачи;

– более высокая результативность относительно используемых на сегодняшний день в ОВД программных продуктов.

Несмотря на имеющиеся проблемы (дефицит в ОВД кадров с навыками программирования и относительная требовательность к оборудованию – необходимость использования видеокарт с технологией *CUDA*), можно сделать вывод о перспективности направления централизованной разработки систем биометрической идентификации на основе *open source* проектов в системе органов внутренних дел Российской Федерации.

Список литературы

1. Прохоренок Н. OpenCV и Java: Обработка изображений и компьютерное зрение. – СПб. : БХВ-Петербург, 2018. – ISBN 978-5-9775-3955-5.
2. Осовский С. Нейронные сети для обработки информации. – М. : Финансы и статистика, 2002.
3. Хайкин С. Нейронные сети: полный курс. – М. : Издательский дом «Вильямс», 2006.
4. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».
5. King D.E. “Dlib-ml: A Machine Learning Toolkit”. – 2009. – pp. 1755–1758.
6. Bradsky G., Kaehler A. “Learning OpenCV”. – O’Reilly, 2008. – ISBN 978-0-596-51613-0.

Титов Павел Михайлович[1]**,**
адъюнкт кафедры уголовного процесса
Уральского юридического института МВД России,

РАССМОТРЕНИЕ УГОЛОВНЫХ ДЕЛ ЧАСТНОГО ОБВИНЕНИЯ СУДАМИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Настоящее время характеризуется как время современных технологий, которые разрабатываются и активно внедряются во все сферы деятельности людей, управления и обороны. Под цифровыми технологиями можно понимать новейшие технические ноу-хау, которые имеют в основе своей направленность на представлении сигналов аналоговых уровней, что способствует повышению качества и переход на новый этап развития цифровой техники. Абстрагируясь от технического определения цифровых технологий, обратим внимание на внедрение цифровых технологий в уголовный процесс России. Обратимся к словам Президента Российской Федерации В. В. Путина, который неоднократно в своих выступлениях подчеркивал, что «у нас есть и кадровый потенциал, и весомый научный задел в этой области. Уверен, что при эффективном и грамотном использовании этих возможностей страна может добиться серьезного прорыва в информационной сфере. Мы просто не должны упустить такой шанс, тем более что ряд государств достигли в этой сфере успеха, имея не такие сильные стартовые позиции» [2]. Данные слова подчеркивают потенциал в данной сфере и обозначают вектор движения дальнейшего развития. Переходя к законодательству и рассматривая его, а также работу по нему посредством контакта граждан и должностных лиц, Т. Н. Москалькова углубленно анализирует перспективны «цифрового законодательства» с внедрением электронного взаимодействия граждан и должностных лиц посредством мессенджеров, чатов или электронных приемных [1], подчеркивает актуальность широкого применения цифровых технологий и в уголовно-процессуальной деятельности. В настоящей статье хотелось бы остановиться на реализации в жизни цифровых технологий, а именно в рассмотрении уголовных дел частного обвинения судами.

Говоря о цифровых технологиях, применяемых в судах, в первую очередь стоит подразумевать видеоконференцсвязь (далее – ВКС), которая широко нашла свое применение, так как ее применение упрощает работу суда с лицами, которые находятся на расстоянии и по тем или иным причинам не явились в зал судебного заседания. Так, А. В. Казакова в статье упоминает об удобстве использования ВКС, но при этом подчеркивает невозможность ее использования, если лицо находится за пределами нашего государства, Российской Федерации [5]. С вышесказанным можно согласиться, так как ВКС, используемая в государственных органах, в том числе и в суде, может применяться только в Российской Федерации, так как имеет определенную степень защиты извне. Многие страны мира на сегодняшний день широко применяют цифровые тех-

нологии в уголовном судопроизводстве в целом и при рассмотрении дел в суде в частности. Это уже не новая практика применения ВКС. Однако можно встретить мало случаев, когда ВКС применяется при рассмотрении уголовных дел частного обвинения. Во-первых, из-за того, что по данной категории дел участвует в самом разбирательстве и поддерживает обвинение частный обвинитель, а не государственный. Во вторых, лица, проходящие по таким делам с любой из сторон, в большинстве случаев не находятся, например, в местах лишения свободы и имеют возможность самостоятельно прибыть в суд. Актуальность ВКС, как нам видится, по делам частного обвинения будет тогда, когда лицо, подавшее заявление, находится в местах лишения свободы или в иных местах, где предстоит провести значительное время. Примером может также служить больница, где человек проходит лечение.

Внимание стоит обратить на критерии допустимости использования цифровых технологий в уголовном судопроизводстве и выделить их: «законность, соблюдение прав и законных интересов личности, актуальность и открытость их применения». При использовании всех цифровых технологий необходимо помнить и о рисках, связанных с их использованием. ВКС технологично имеет свою степень защиты, но в настоящее время на месте ничего не стоит и все бурно развивается, в том числе и средства противодействия. Поэтому применяя цифровые технологии, в том числе и при рассмотрении уголовных дел частного обвинения по существу, необходимо обращать внимание на методы защиты применяемых цифровых технологий, которые должны не просто упростить работу суда, но и главным образом не навредить, особенно от разглашения сведений, охраняемых законодательством Российской Федерации. Слабые стороны цифровизации уголовного судопроизводства с позиции механизма правового регулирования раскрываются в статье С. В. Зуева и А. С. Титовой [4]. Однако на слабые стороны всегда найдутся сильные, которые покажут жизнеспособность и применяемость. Л. В. Головко с осторожностью относится к цифровизации уголовного судопроизводства в целом и обращает внимание на то, «что самый мощный научно-технологический прорыв в истории человечества 20–60-х гг. прошлого века не привел к созданию «космического уголовного процесса» или «лунной подследственности» [3]. С данной осторожностью можно согласиться, так как цифровизация, в первую очередь, должна быть безопасной.

Таким образом, используя цифровые технологии при рассмотрении уголовного дела частного обвинения, необходимо обращать внимание на защиту данных. При этом широкое использование данных технологий ускоряло бы рассмотрение уголовных дел, не способствовало бы затягиванию самого рассмотрения и в конечном итоге приводило бы к более оперативному и всестороннему рассмотрению уголовного дела.

Список литературы

1. Выступление Президента Российской Федерации на расширенном заседании коллегии Генеральной прокуратуры Российской Федерации 19 марта 2019 г. [Электронный ресурс] // URL: https:// kremlin.ru (дата обращения: 15.11.2019).

2. Выступление Президента Российской Федерации на совещании по вопросам развития информационных технологий [Электронный ресурс] // URL: http:// kremlin.ru/events/president/transcripts/22777 (дата обращения: 15.11.2019).

3. Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция // Вестник экономической безопасности. – 2019. – № 1. – С. 15–25.

4. Зуев С. В., Титова А. С. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства // Правопорядок: история, теория, практика. – 2019. – № 1 (20). – С. 49–54.

5. Казакова А. В. Новые технологии в Российском уголовном процессе // Юридический вестник Самарского университета. – 2017. – № 3. – С. 94–95.

Федосеева Елена Леонидовна[1]**,**
доцент кафедры уголовного процесса
Уральского юридического института МВД России,
кандидат юридических наук

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ И ВЕРСИИ, ВЫДВИГАЕМЫЕ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В связи с развитием технического прогресса, компьютеризацией общества и повсеместным распространением в обиходе глобальной сети Интернет в стране возникла потребность в использовании компьютерной техники и различного рода электронных устройств обмена и передачи информации.

По данным компании «TNS Россия», 73 % из числа опрошенных граждан пользуются электронными деньгами минимум раз в год, почти 50 % – раз в месяц и чаще. Определены 5 самых популярных категорий платежей электронными кошельками: интернет-покупки, сотовая связь, денежные переводы, коммунальные услуги, цифровой контент [1]. Увеличение потребления в стране электронных ресурсов во многих сферах общественных отношений повлекло за собой появление и рост преступлений в области компьютерной информации. Между тем анализ статистики поступающих в суды уголовных дел по преступлениям, предусмотренным гл. 28 УК РФ, свидетельствует о незначительном их количестве по данным составам преступлений. Так, в 2018 г. за данные преступления было осуждены 129 человек [2]. Указанное обстоятельство заставляет задуматься об уровне эффективности выявления и расследования таких преступлений.

По результатам статистического опроса сотрудников правоохранительных органов и судов на тему уголовно-правового противодействия киберпреступлениям [3], на вопрос о том, испытывают ли практики трудности при квалификации и расследовании компьютерных преступлений, 60 % ответили, что испытывают, и 40 % затруднились с ответом. Сложность в понимании способов совершения компьютерных преступлений и в их расследовании представляет, в том числе, используемая в данной сфере терминология, поскольку она имеет технический характер. Большинство понятий определяются и содержатся в отраслевых и специальных нормативных актах. Указанные обстоятельства не позволяют сформировать единую практику применения положений гл. 28 УК РФ.

В ходе расследования данного рода преступлений подлежат установлению, а в дальнейшем доказыванию такие обстоятельства как: факт создания и использования вредоносных программ, несанкционированного доступа к компьютерной информации; место и время несанкционированного проникновения в систему или сеть; надежность средств защиты компьютерной информации; способ совершения преступления; лица, совершившие, их виновность и мотивы; последствия неправомерного доступа к компьютерной информации; обстоятельства, способствовавшие созданию и использованию вредоносных программ и др.

На первоначальном этапе расследования версии совершенного преступления могут быть как общие, так и частные. Выдвигаются следующие общие версии: преступление имело место при тех обстоятельствах, которые подтверждены материалами проверки; заявление о преступлении ложное (преступление было инсценировано). Частные версии касаются обычно личности преступника, мотивов совершения преступления, способов несанкционированного доступа или создания и использования вредоносных программ, размера причиненного ущерба и т. д.

Далее необходимо разобраться со следственными ситуациями, возникающими на данном этапе расследования. Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного сотрудника.

На момент принятия решения о возбуждении уголовного дела возможны три типичные следственные ситуации. Первая связана с отсутствием сведений о совершенном преступлении и о лице, его совершившем. Вторая ситуация возникает, когда не установлена личность преступника, но имеются сведения об объективной стороне преступления. В последней ситуации обстоятельства совершенного преступления нам известны, лицо, совершившее противоправное деяние, установлено (последняя ситуация возникает в условиях очевидности, когда большинство обстоятельств известно).

В условиях первой и второй следственных ситуаций целесообразно проводить процессуальные, следственные действия, направленные на сбор доказательств и привлечение лица к уголовной ответственности. Наибольшую важность здесь имеют поисковые мероприятия, направленные на установление лица, совершившего преступление. В таком случае следователь направляет в орган дознания (например, в отдел «К») поручение о производстве оперативно-разыскных мероприятий в целях установления способа совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств. Планирование дальнейших следственных действий производится в зависимости от информации, полученной при реализации вышеуказанных мероприятий.

В следующей (третей) ситуации в условиях очевидности, когда известны все обстоятельства преступления и личность преступника, целесообразно приведение таких групп следственных и процессуальных действий, как: осмотр места происшествия. Сложность проведения данного следственного действия вызвана проблемой определения мест, в которых располагался злоумышленник, если подключался к динамичному IP-адресу. Необходимо помнить о том, что преступники для осуществления своей незаконной деятельности могут использовать различные методы и способы для затруднения их обнаружения. Например, использование *VPN* (это технология, которая обеспечивает зашифрованное соединение поверх интернет-соединения), которое значительно затрудняет, а порой и вовсе делает невозможным произвоство расследования по уголовному делу.

Если место совершения преступления определить на данном этапе не представляется возможным, то целесообразно осмотреть место жительства заявителя, его рабочее место. Провести осмотр предметов и документов, в том числе электронных носителей информации, электронных документов, электронных сообщений, сайта или страницы в сети Интернет. Производство осмотра целесообразно проводить с участием специалиста. Использование криминалистической техники при этом, во избежание разрушения носителей компьютерной информации и микросхем памяти, должно быть согласовано со специалистом [4].

Согласно ст. 164.1 УПК РФ (введена Федеральным Законом от 27 декабря 2018 г. № 533-ФЗ) [5], по общим правилам изъятие носителей информации не допускается. Исключением является наличие постановления о назначении экспертизы в отношении электронных носителей информации. После изъятия компьютерной техники необходимо собрать доказательства, указывающие, что этой техникой в определенное время пользовался подозреваемый.

При установлении и задержании подозреваемого производится его допрос. При подготовке к допросу необходимо: изучить материалы дела, определить очередность проведения допросов; предварительно изучить личность допрашиваемого; получить консультацию специалиста и составить план допроса. Для выбора тактики допроса и определения круга вопросов, следует получить сведения о лице по месту жительства, учебы, работы, досуга.

Большое значение имеет производство экспертных исследований. Чаще всего проводится судебная компьютерно-техническая экспертиза, которую можно определить как регламентированное законом исследование компьютерной информации, технических средств, программного обеспечения компьютерной системы, проводимое с целью получения информации, имеющей значение для уголовного дела.

Далее должностному лицу, осуществляющему расследование, предстоит анализ полученной информации и решение вопроса о привлечении лица в качестве обвиняемого. Виды следственных, процессуальных действий и оперативных мероприятий, их последовательность и процедура производства должны определяться каждой конкретной следственной ситуацией, складывающейся по уголовному делу.

Таким образом, при расследовании данной категории преступлений практики сталкиваются с проблемами организации и проведения проверки сообщений о преступлении, а в дальнейшем с вопросами производства следственных действий, направленных на обнаружение, изъятие, осмотр компьютерной техники и электронных носителей информации. В большей степени проблемы вызваны недостаточной правовой регламентаций порядка производства по уголовным делам, что значительно осложняет деятельность по раскрытию и расследованию компьютерных преступлений. Кроме того, деятельность должностных лиц, осуществляющих раскрытие и расследование компьютерных преступлений, требует серьезного совершенствования (повышения квалификации).

Указанные выводы подтверждают необходимость разработки четкого алгоритма действий должностных лиц правоохранительных органов, сталкивающихся с организацией расследования в борьбе с киберпреступностью.

Список литературы

1. Шангараев Р. Н. Национальная платежная система в контексте экономической безопасности Российской Федерации / Р. Н. Шангараев, Е. В. Лобас, И. В. Трифонов // Вестник Московского университета МВД России. – 2016 – № 6. – С. 146.

2. Данные Агентства правовой информации [Электронный ресурс] // URL: http://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 12.11.2019).

3. Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных техно-логий : дис. … канд. юрид. наук. – Краснодар, 2016. – С. 215.

4. Чистова Л. Е. Расследование преступлений в сфере незаконного оборота сильнодей-ствующих или ядовитых веществ : монография. – М. : Юрлитинформ, 2014. – С. 48.

5. Уголовно-процессуальный кодекс Российской Федерации (ред. от 03.07.2019) [Электронный ресурс] // URL: https://www.consultant.ru.

Чипурина Елена Александровна[1]**,**
доцент кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

УЧЕТ ЛИЧНОСТИ ПРЕСТУПНИКА В ПРЕДУПРЕЖДЕНИИ КИБЕРПРЕСТУПЛЕНИЙ

Как отмечается в СМИ, за последнее десятилетие количество киберпреступлений значительно увеличилось и продолжает расти. Если в 2013 г. было зарегистрировано всего 11 тыс. таких преступлений, то за первые восемь месяцев 2019 г. в России было зарегистрировано 180 153 киберпреступления. Это на 66,8 % больше показателя за аналогичный период предыдущего года.

Киберпреступления становятся все более изощренными и причиняют колоссальный ущерб гражданам и организациям разных государств. По оценкам экспертов, в России киберпреступники наносят ущерб более чем на 2,2 млрд долларов в год. Глобальные же потери от кибератак в 2017 г. составили 172 млрд долларов.

И хотя эти преступления совершаются в виртуальном пространстве, за каждым из них стоит вполне реальный преступник или группа преступников, которые должны преследоваться по закону.

А между тем, в обществе до сих пор киберпреступник воспринимается как положительный герой, своего рода виртуальный Робин Гуд, который взламывает кошельки богачей. На самом же деле хакеры с одинаковым энтузиазмом опустошают счета и крупных компаний, и простых пользователей. И пока никто не был замечен в использовании похищенных средств в благотворительных целях.

Виртуальные преступники могут совершать за одну секунду тысячу преступлений по всему миру, и при этом они практически неуловимы.

Так кто же они – современные киберпреступники?

Если отталкиваться от понятия киберпреступность, под которой понимается преступная деятельность, осуществляемая с использованием компьютеров и (или) через сеть Интернет, киберпреступник – это лицо, совершающее уголовно наказуемые деяния с использование компьютеров и (или) через сеть Интернет. Личность же киберпреступника – это совокупность социально-демографических, нравственно-психологических и уголовно-правовых свойств личности, определяющих преступное поведение индивида, выражающееся в совершении киберпреступлений[2].

Однако в том же Интернете при попытке собрать информацию о киберпреступниках мы постоянно сталкиваемся с понятием «хакер». Хакер – это более широкое понятие, многозначный термин в области вычислительной техники и программирования.

---

[1] © Чипурина Е. А., 2019.

[2] Афанасьева О. Р., Шиян В. И., Гончарова М. В. Криминология и предупреждение преступлений : учебник и практикум для СПО. М. : Юрайт, 2019. С. 331.

На начальном этапе развития глобальной сети Интернет в 60-е гг. XX в. зарождавшееся в американской молодежной среде движение хакеров не носило деструктивного характера. Это была демократическая и творческая среда. Хакеры, как и хиппи, выступали сторонниками неограниченной свободы, но применительно к киберпространству.

С конца XX в. хакеры стали ассоциироваться с «компьютерными взломщиками», т. е. программистами, злонамеренно обходящими системы компьютерной безопасности. Хотя в профессиональной сфере IT-специалистов подобных людей называют «кракерами» (англ. *cracker* – взломщик) – людьми, обходящими системы безопасности компьютерных устройств.

Есть «правильные» хакеры, которые занимаются изучением систем безопасности, а не взломами. Они создают полезные бесплатные софты, учат других решению проблем с компьютерами, т. е. помогают людям.

А есть и другие – попросту взломщики, т. е. люди, которые применяют свои знания для достижения меркантильных целей. Они взламывают корпоративные системы, воруют деньги с электронных счетов, создают и распространяют компьютерные вирусы.

В исследованиях деятельности хакеров доминируют два подхода.

Первый из них на основе критерия несанкционированного вторжения в информационную систему отождествляет хакерство с преступной деятельностью. По данному критерию хакеров можно классифицировать следующим образом:

– «шутники» – взламывают компьютерные системы для достижения известности. Стараются не причинять серьезный вред системе. Вносят различные юмористические заставки или вирусы с различными визуально-звуковыми эффектами;

– «фрикеры» – осуществляют взлом телекоммуникационных сетей, которые передают голос, т. е. они подключаются к телефонным, сотовым, спутниковым сетям для осуществления международных переговоров. Для «потребителей» этой услуги цена разговора снижается в несколько раз по сравнению с официальной. Счет же от компании получает абонент, чье оборудование было использовано (взломано). По данным МВД в Москве, с каждой такой точки ежедневно получают от 500 долларов прибыли. Удешевление связи привело к снижению количества данных правонарушений;

– «сетевые хакеры» – взламывают интрасети в целях получения новых знаний о типологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, о методах защиты;

– «взломщики-профессионалы» – взламывают компьютерные системы с целью кражи или подмены хранящейся там информации. Они характеризуются системностью и организованностью действий. К этой категории относятся взломщики программного обеспечения, специалисты по подбору паролей;

– «вандалы» – взламывают с целью разрушения компьютерной системы, портят или удаляют данные, создают вирусы[1].

[1] Скородумова О. Б. Хакеры как феномен информационного пространства [Электронный ресурс] // URL: http// ecsocman.hse.ru/data /679/735/1231/009.SKORODOUMOVA.pdf.

Второй подход опирается на критерий мотивации при оценке деятельности хакеров: «человек, подсматривающий и ищущий (хакер) становится взломщиком, действующим корыстно (кракер), беспредельно разрушительно (кибертеррорист) или идейно (хактивист)».

Закрытость хакерского сообщества приводит к тому, что мы не можем получить полные и достоверные сведения о личности хакеров. Хотя и существуют отдельные исследования личности компьютерного преступника.

Тем не менее, исходя из особенностей данной субкультуры, мы можем говорить о некотором постоянстве отдельных ее характеристик.

Проводимые ранее исследования показывают, что подавляющее большинство киберпреступников – мужчины (около 96 %).

Распределение преступников по возрасту выглядит следующим образом: до 18 лет – 29,9 %; от 18 до 24 лет – 60,4 %; старше 24 лет – 9,7 %. Средний возраст преступника – около 22 лет. За прошедшие 15 лет процент преступников, не достигших 18 лет, вырос почти в 2 раза, т. е. преступность сильно «помолодела».

Постоянное место работы имеет 31,3 % лиц, но лишь у 13,9 % из выявленных лиц работа связана с обслуживанием компьютеров.

Обучаются в высших учебных заведениях 38,2 %: из них 25,7 % – на технических специальностях, так или иначе связанных с компьютером; 14,6 % – подростки, обучающиеся в школах.

На момент совершения противоправных действий с родителями проживало почти 80 % лиц.

С домашнего компьютера были совершены 93 % деяний.

Полученная информация свидетельствует, что раскрываются наиболее простые и менее общественно опасные деяния.

Предприняты первые попытки сформировать обобщенный портрет русского хакера. Согласно данным экспертно-криминалистического центра МВД России, русский хакер – это подросток или мужчина в возрасте от 15 до 45 лет, как правило, не привлекавшийся к уголовной ответственности; владеющий компьютером в диапазоне от начального до высокопрофессионального уровня; добросовестный работник, но с завышенной самооценкой, нетерпимый к насмешкам, потере социального статуса; отличается ярко выраженной индивидуальностью, обычно скрытен, любит уединенную работу, малообщителен. Русские хакеры в большей степени предрасположены к идеологическому обоснованию взломов, чем их собратья за рубежом[1].

Особого внимания заслуживают хакеры-женщины. Как было уже указано выше, они составляют не многочисленную группу – от 4 до 6 %. В среднем хакерам-женщинам около 35 лет, они обладают более скромными познаниями в компьютерах и взламывают компьютерные системы при помощи более слабой вычислительной техники, чем хакеры-мужчины. Всего 5 % хакеров-женщин знали, что они совершают незаконный поступок. Но более чем половина стре-

[1] Вершинин М. Современные молодежные субкультуры: хакеры.

милась к получению именно экономической прибыли. Женщины чаще входят в состав мужской преступной группы.

На сегодняшний день участниками (соучастниками) кибердеяний являются не только хакеры-профессионалы, но и различного рода мошенники, вымогатели, рэкетиры, террористы, сутенеры, педофилы, торговцы людьми, оружием, боеприпасами, наркотиками.

Умысел киберзлоумышленников все чаще нацеливается не только на незаконное обогащение, получение финансовых средств неправовыми способами, но и на достижение политических и др. целей (например, в ходе избирательной кампании могут преследоваться цели «цветных революций»).

Высокая латентность, рост числа киберпреступников, совершенствование информационных технологий требуют соответствующих подходов к противодействию данному виду преступности.

В рамках международного сотрудничества необходима более активная консолидация усилий правоохранительных органов различных государств не только в осуществлении международного розыска и регистрации преступников, но и создании доступной для компетентных органов картотеки лиц, «замеченных» в совершении противоправных действий в киберпространстве.

Правовой подход в предупреждении преступлений предполагает разработку уголовно-правовых норм, предусматривающих ответственность за новые виды киберпреступлений.

Больше внимания следует уделять организационному подходу, а именно совершенствованию организационных и профилактических мероприятий.

В этом направлении может помочь использование результатов различных исследований личностных особенностей киберпреступников. Известно, что киберпреступники нередко страдают аутистическими расстройствами, например синдромом Аспергера, при котором имеют место нарушения развития, связанные с серьезными трудностями в социальном взаимодействии, а также ограниченным, стереотипным, повторяющимся набором интересов и занятий[1]. Имея такую информацию, мы можем, во-первых, активнее выявлять латентных киберпреступников, взаимодействия с медицинским персоналом профильных медицинских учреждений, а во-вторых, вовлекать лиц с психическими особенностями в другие виды правомерной деятельности.

Таким образом, дальнейшее исследование характеристик отдельных типов личности киберпреступников весьма актуально для повышения эффективности противодействия киберпреступности.

[1] Афанасьева О. Р., Шиян В. И., Гончарова М. В. Криминология и предупреждение преступлений. С. 331.

Бельдеубаева Даяна Ренатовна[1]**,**
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Екатерина Николаевна[2]**,**
доцент кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ПЕРСПЕКТИВЫ ТЕХНОЛОГИИ ВИЗУАЛИЗАЦИИ СИГНАЛОВ ГОЛОВНОГО МОЗГА

Вернуть возможность движения людям, потерявшим конечности или утратившим способность двигаться, – одна из актуальных задач мирового медицинского сообщества. Благодаря интерфейсу «мозг-компьютер» (ИМК) или нейрокомпьютерному интерфейсу – новой технологии, которая позволяет человеку воздействовать на окружающую среду усилием мысли – через расшифровку мысленных команд по сигналам в электроэнцефалограмме (ЭЭГ) или другим методам записи активности мозга, человеку предоставляется возможность реализовать свои потребности в движении путем внешних устройств: манипулятором, роботом, инвалидной коляской, курсором в компьютерной программе и т. п. Люди ограниченных возможностей – и не только они – в дальнейшем смогут общаться с внешней средой через ИМК.

Рис. 1. Схема, иллюстрирующая принципы технологии интерфейса «мозг-компьютер»

Принцип технологии ИМК построен на основе 5 компонентов (*рис. 1*):

1. регистрация ЭЭГ;
2. препроцессинг и анализ полученных данных;
3. выделение признаков;
4. классификация (распознавание) сигналов головного мозга;
5. управление внешним устройством.

Биологические аспекты

Электрическую активность в головном мозге собирают по данным ЭЭГ (электроэнцефалографа). ЭЭГ – это неинвазивная технология, которая регистрирует скоординированную электрическую активность в больших группах нейронов через сеть электродов, которые обычно носят в шапочке, которая подходит для головы человека.

Рис. 2. 3D-модель головного мозга, полученная по данным магнитно-резонансной томографии (МРТ)[1]

На *рис. 2* приведен пример электрической активности головного мозга. Золотые волокна на изображении – это миелинизированные группы нервных аксонов, называемые белым веществом. Эти пучки аксонов соединяют и координируют связь между различными областями мозга. Сигналы, которые проходят через пучки аксонов, визуализируются в виде импульсов света.

Различные цвета, которые приходят и уходят на протяжении всей визуализации, отслеживают активность в различных частотных диапазонах (иногда называемых «мозговые волны»). Яркость цвета указывает на интенсивность активности в определенной полосе частот. Модель отслеживает активность в тета-, бета- и альфа-диапазонах частот:

1. Тета, показанная красным цветом, представляет собой низкочастотный диапазон (от 4 до 7 Гц), который обычно наблюдается при сонливости или медитации у детей старшего возраста и взрослых.

2. Бета, показанная зеленым цветом, представляет собойдиапазон от низкого до среднего уровня (от 16 до 31 Гц), который связан с различными психическими состояниями и физической активностью. Например, бета может уменьшаться во время активных движений и увеличиваться во время тревожного мышления.

3. Альфа, показанная синим цветом, представляет собой еще один низкочастотный диапазон (от 8 до 15 Гц), который обычно связан с релаксацией или закрытием глаз.

4. Цветовые смеси проявляют активность в более чем одной полосе. Например, фиолетовый показывает активность как в тета-, так и в альфа-диапазонах.

---

[1] Визуализация продемонстрирована в *Glassbrain Flythrough 2015*, который был представлен на видеоконкурс *Science's Data Stories*.

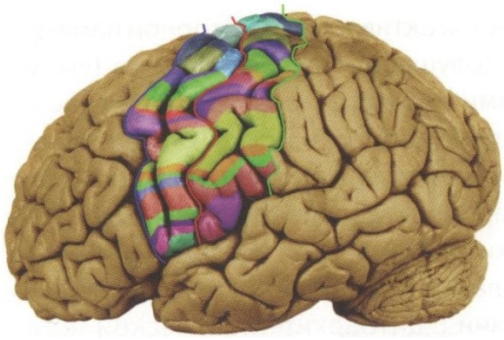

Рис. 3. Сенсомоторный центр мозга человека в общем плане

Кора больших полушарий мозга играет ведущую роль в мозговой организации психических процессов.

Существуют функционально специализированные участки коры головного мозга, отвечающие за различные органы чувств. В рамках рассматриваемой проблемы затрагиваются сенсомоторные центры.

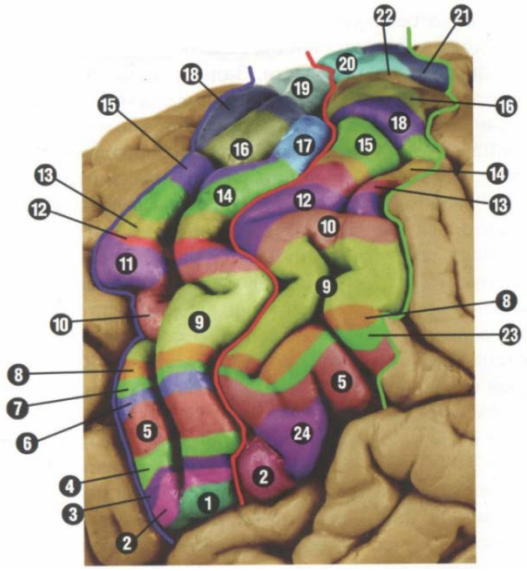

Рис. 4. Сенсомоторные центры мозга человека: 1) корень языка; 2) гортань; 3) нёбо; 4) нижняя челюсть; 5) язык; 6) нижняя часть лица; 7) верхняя часть лица; 8) шея; 9) пальцы руки; 10) кисть; 11) рука от плеча до кисти; 12) плечо; 13) лопатка; 14) грудь; 15) живот; 16) голень; 17) колено; 18) бедро; 19) пальцы ноги; 20) большой палец ноги; 21) четыре пальца ноги; 22) стопа; 23) лицо; 24) глотка. Между синей и красной линиями лежат моторные центры коры, а между красной и зеленой линиями – сенсомоторные.

Наконец, основная мозговая активность, связанная с движением руки, находится в диапазоне от 7 до 30 Гц.

Анализ данных

К основным объектам изучения в сигнале электроэнцефалограммы относятся движение глаз, движение электродов, сокращения мышц головы и сердца, сетевая помеха в 50–60 Гц. Помехи, вызванные движением глаз, электродов и мышц, в сравнении с полезным сигналом, располагаются в области более низких частот – от 0,1 Гц до 6 Гц. Используется полосовой фильтр с полосой пропускания от 7 до 30 Гц. Важно, чтобы цифровая фильтрация вносила наименьшие искажения в сигнал, поэтому был выбран фильтр с конечной импульсной характеристикой.

Что касается децимации – понижения частоты дискретизации данных, то ее понизили с 500 до 62,5 Гц. Поскольку максимальная полезная частота составляет 30 Гц, то, учитывая теорему Найквиста, частота дискретизации должна быть больше 60 Гц.

Выявление и классификация признаков сигнала головного мозга

Учеными, исследователями используются разные методы выделения характерных признаков сигнала. Это необходимо для сокращения количества входных данных, исключения лишнего и повышения точности классификации сигналов головного мозга. Среди испробованных методов были: метод главных компонент [1], выбор электродов с точки зрения биологии [2] и вейвлет-преобразование [3].

Но большинству исследователей пришлось отказаться от метода главных компонент, потому что при вычислении обязательной в данном способе матрицы с помощью *SVD* (*singular value decomposition* – сингулярного разложения) предполагается, что глубинные сигналы мозга взаимно ортогональны. А они, судя по результатам экспериментов, не взаимно ортогональны. Кроме этого, количество датчиков в нашем эксперименте сводилось к 32, что не является достаточным для хорошей *SVD*. Для неортогональных сигналов нужно использовать *ICA* (*independent component analysis*) – метод независимых компонент. *ICA* мы не успели попробовать.

При выборе электродов опираются на их пространственное расположение. Электроды, с которых предоставлялись данные, на следующем рисунке помечены цифрами от 1 до 32 (*рис. 5*).

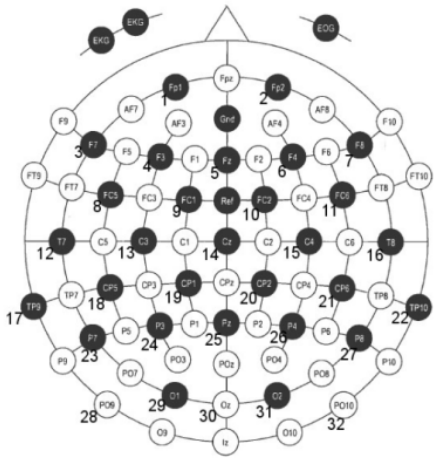

Рис. 5. Схематическое изображение электродов
на поверхности головы

Выбрав нужные электроды, сосредоточиваются на вейвлет-преобразовании в качестве выделения необходимых характерных признаков. Существует негласный принцип выбора вейвлета: вид базовой вейвлет-функции должен быть схожим с характерным обрабатываемым сигналом (*рис. 6*). Данный способ позволяет анализировать «тонкую» структуру сигналов за счет одновременной локализации и по частоте, и по времени.

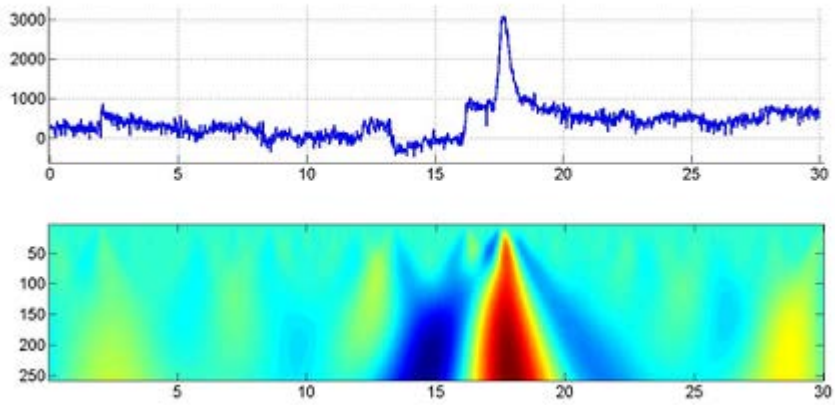

Рис. 6. Результат вейвлет-преобразования для сигнала *EEG*

Классификация (распознавание) сигналов головного мозга

Сверточные нейронные сети – это один из наиболее востребованных вариантов нейронных сетей, который уже зарекомендовал себя с двумерными сигналами (например, изображениями). Однако такие сети могут работать и с одномерными сигналами.

С помощью сверточной нейронной сети было выявлено, что 4 096 отсчетов (до децимации) дают наименьшую вероятность ошибки в конечной модели. Полученная модель позволила нам получить площадь под кривой *ROC*, равную 0,91983.

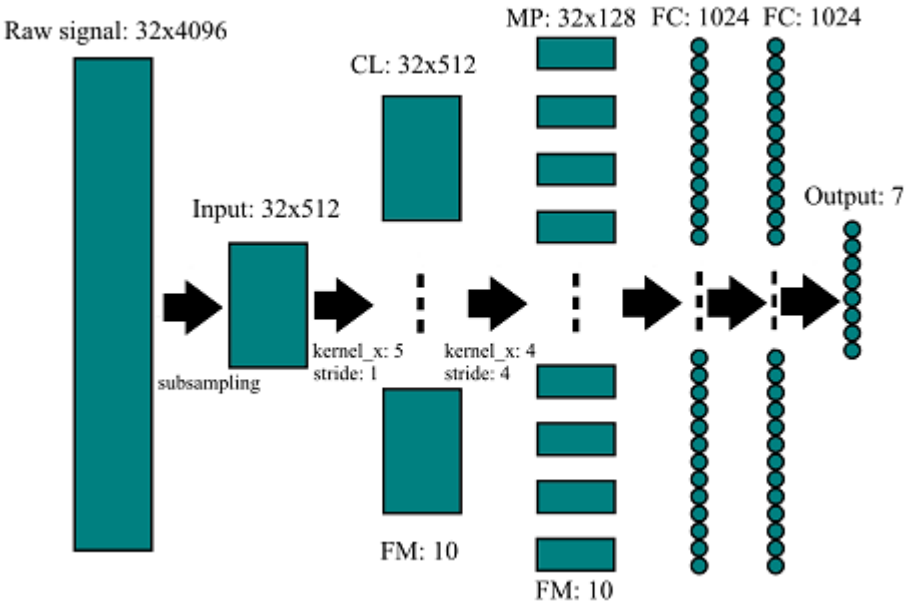

Рис. 7. Полученная модель: *CL* – сверточный слой, *MP – map pooling*, *FC* – полносвязный слой, *FM* – количество масок с характерными признаками, *kernel_x* – размер ядра, *stride* – размер шага.

Вторым исследуемым алгоритмом стали «случайные деревья» или «случайный лес», поскольку на сегодня этот способ является одним из самых популярных в области классификации. Алгоритм состоит из ансамбля решающих деревьев, для каждого из которых из общей выборки генерируется своя выборка. Третьим алгоритмом машинного обучения, выбранным нами для исследования, стали *RNN* или рекуррентные нейронные сети. Это нейронные сети,

в которых есть обратные связи. Биологические нейронные сети являются рекуррентными. В них есть память, что позволяет не подавать историю сигнала в сеть.

Множество опытов с рекуррентной нейронной сетью, разные архитектуры и задержки в обратных связях приводят к необучаемостью сети. Возникают проблемы с памятью – не удается создать сложную сеть с числом слоев более двух. Тогда исследователи пришли к выводу, что нужно использовать специальный вид нейронных сетей *LSTM* (*Long Short Term Memory*). Тем не менее сложность *LSTM* алгоритма предполагает гораздо более глубинное исследование, чем позволяли условия конкурса.

Выводы

В результате проведенных опытов получила высокое качество классификации сигналов головного мозга в процессе движения руки. Благодаря метрике качества «площадь под кривой *ROC*», полученной в результате использования сверточных нейронных сетей, мы убедились в эффективности алгоритмов глубинного обучения в классификации сигналов различного рода.

Это позволяет с уверенностью заключить, что сверточные нейронные сети – один из лучших существующих на сегодня методов машинного обучения для создания нейрокомпьютерного интерфейса.

Список литературы

1. Бухарин С. В. Алгоритм выделения главных компонент с помощью самоорганизующейся нейронной сети хебба / С. В. Бухарин, А. В. Мельников, В. В. Навоев // Вестник Воронежского института МВД России. – 2015. – № 2.

2. Омаров Т. З. Концепция искусственной нейронной сети // Современные научные исследования и инновации – 2016. – № 5 [Электронный ресурс] // URL: http://web.snauka.ru/issues/2016/05/66203 (дата обращения: 25.03.2019).

3. Яковлев А. Н. Введение в вейвлет-преобразования : учебное пособие. – Новосибирск : Изд-во НГТУ, 2003.

Рудакова Наталия Константиновна[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Екатерина Николаевна[2]***,***
доцент кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ВЫЯВЛЕНИЕ ПРИЗНАКОВ ГРУПП ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В СЕТИ ИНТЕРНЕТ

В современное время экстремистская и террористическая деятельность создает реальную угрозу жизнедеятельности государства, посягает на конституционные права и свободы граждан Российской Федерации, общественную безопасность и общественный порядок. Масштаб проблемы экстремизма и терроризма показывает тот факт, что им отводятся отдельные места в Стратегии национальной безопасности Российской Федерации до 2020 г.

Развитие компьютерных технологий и электронных средств массовой информации повлекло формирование единого мирового информационного пространства, которое открыло новые возможности противоборствующим сторонам.

Информационное противоборство реализуется в форме психологических операций, использующих специальные методы, способы и средства манипулирования общественным сознанием. На сегодняшний момент создана большая технологическая база, посредством которой государственные органы выявляют и расследуют преступления, связанные с противоправными и деструктивными информационными воздействиями, в том числе и экстремисткой, а также террористической деятельностью.

Рассматривая тенденцию увеличения распространенности экстремистской и террористической деятельности в интернет-среде, можно сделать вывод об актуальности рассматриваемой темы.

Основная форма распространения экстремистской и террористической информации осуществляется через тексты: статьи, печатные издания, стихи, песни, а также комментарии интернет пользователей. В последнее время все больше интернет-пространство занимают видеоролики, видеофильмы экстремистского содержания.

Для обнаружения наличия или отсутствия в этих материалах признаков экстремизма используется совокупность научных методов. В исследовании, прежде всего, текстовых материалов используются контент-анализ, дискурс анализ и контекстуальный (контекстный) анализ.

Для анализа содержания плакатов, фотографий, картин, карикатур и других объектов с изображениями целесообразно использовать визуальное исследова-

ние (метод фотографирования). Проблематика многообразия жанров, с помощью которой выражаются идеи экстремизма, актуализирует проблему выбора методов анализа интернет материалов.

Наиболее распространенным является в изучении текстов контент-анализ. Однако функции и возможности этого метода не в полной мере позволяют выявить признаки экстремизма, в частности, скрытой его формы. В том виде, в которой понимается содержание этого метода (количество упоминаний слов, словосочетаний) и используется на практике, не охватывает всего многообразия проявления экстремизма (политического экстремизма), не в полной мере позволяет выявить его признаки. Более того, выявление признаков экстремизма предполагает исследование содержания текста, где для этой цели используется контекстуальный (контекстный) метод.

При выборе метода анализа интернет материалов с признаками экстремизма (политического экстремизма), важно знать, что контент-анализ вскрывает содержание текста, но не способен интерпретировать значение этого содержания, и поэтому исследователь должен изучать текст непосредственно. Поэтому в исследовании материалов с экстремистским или террористическим содержанием контент-анализ следует рассматривать только как дополнение других методов.

Обычно в группах экстремистской и террористической направленности применяются техники психологического воздействия, которые в сочетании со спецификой психологии человека и его информационной средой дают повышенный эффект. А также, исходя из специфики интернет-среды и изучая материалы исследований государственных органов по выявлению сообществ подобной направленности в информационно-коммуникационных сетях, предоставляется возможность выделения следующих основных признаков, указывающих на принадлежность групп к экстремистской и террористической деятельности:

1) представляют собой сообщества, в которых целенаправленно применяются техники насильственного психологического воздействия и формируется социально-психологическая зависимость;

2) имеют сплоченных адептов, которые укрепляют веру друг друга в правильность собственных действий и подталкивают к дальнейшему участию;

3) имеют подобие идеологии, которое выражается в отношении к окружающему миру. В некоторых группах имитируется примитивное представление о потустороннем мире;

4) культивируется избранность. Те, кто состоит в группе – выше остальных;

5) имеют место ритуалы и правила, единые для всех членов сообщества, обязательные обряды;

6) появляются объекты фанатичного поклонения;

7) организаторы стремятся сократить и вытеснить из жизни подчиняемого лица влияние семьи и других значимых людей, не входящих в группу. Цель – овладеть их социальным пространством;

8) имеется общая символика и сленг, значение которого понятно ограниченному кругу людей и служит своеобразным идентификатором для разделения «свой-чужой». Такая атрибутика свойственна многим группам;

9) кураторы, как и лидеры, стремятся осуществлять контроль над иными сферами жизни участника вне группы;

10) требуют сокрытия компрометирующей сообщество информации. Все люди и сообщества при общении стараются преподносить себя в лучшем свете, однако запрет на нелицеприятную информацию часто является обязательным;

11) активно эксплуатируют людей с кризисами и травмами, предлагая пути решения проблем.

Итак, благодаря данной характеристике, мы можем однозначно понять: относится ли обнаруженный контент в сети Интернет к материалам, содержащим информацию террористической и экстремистской направленности.

Таким образом, можно сделать вывод о том, что с развитием информационно-коммуникативных технологий и повсеместному распространению Интернета, экстремизм и терроризм из локального характера переросли в глобальный. Благодаря этому, экстремизм и терроризм параллельно существуют, как в реальном мире, так и в виртуальном, приобретая конкретные очертания и проявления в реальности.

Возможности социальной сети позволяют размещать материалы разного жанра, а также их быстрое распространение методом «снежного кома» или же «цепной реакции, «через репост». Тем самым достигая желаемого результата за очень короткое время на относительно большой аудитории.

Список литературы

1. Кафтан В. В. Противодействие терроризму. – М. : Юрайт, 2016.
2. Овчинский С. С. Оперативно-розыскная информация : монография / под ред. А. С. Овчинского. – 2-е изд., доп. – М. : ИНФРА-М, 2017.
3. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс] // URL: https://42.мвд.рф/экстремизм-и-экстремистская-деятельность.

Боровиков Валерий Борисович[1]**,**
профессор кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент,
заслуженный сотрудник ОВД России

Боровикова Виктория Валерьевна[2]**,**
доцент кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ОБ УЧЕТЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ДЛЯ КОНСТРУИРОВАНИЯ НОРМ ОСОБЕННОЙ ЧАСТИ РОССИЙСКОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА

Информационные технологии активно используются в различных сферах современной цивилизации, в том числе при совершении различных преступлений. Это неслучайно, поскольку их применение в значительной мере увеличивает деструктивные возможности многих общественно опасных посягательств, нарушающих уголовный закон.

Законодатель в целом правильно реагирует на названную выше тенденцию в структуре и динамике преступности. Уже сейчас, по нашим подсчетам, около 30 статей УК РФ, включая указанные в гл. 28 УК РФ «Преступления в сфере компьютерной информации», содержат прямые указания на использование электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) в качестве признаков основного или квалифицированного состава преступления (см., например, п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 3 ст. 137, п. «в» ч. 2 ст. 151.2 УК РФ)[3]. Но это еще не все. В отдельных случаях закон применяет более широкую формулировку – «с использованием средств массовой информации» (например, ст. 137, ч. 2 ст. 128.1 УК РФ), которая также не исключает использование при совершении преступлений различных информационных технологий. Если руководствоваться этим подходом, то число преступлений, допускающих использование подобных технологий еще более увеличивается (примерно до 40).

Таким образом, можно прийти к выводу, что широкое распространение информационных технологий отражается на состоянии современной преступно-

---

[1] © Боровиков В. Б., 2019.

[2] © Боровикова В. В., 2019.

[3] Подтверждением общественной опасности деяний, связанных с использованием информационных технологий, свидетельствует хотя бы такой факт: за 9 месяцев 2017 г., по данным Управления «К» МВД России, сотрудники этого подразделения обнаружили свыше 200 тыс. «самоубийственных» публикаций в социальных сетях (Фалалеев М. В. «Группе смерти» прием закрывается // РГ. – 2017. – 10 окт.).

сти, увеличивает возможности совершения различных преступлений и заставляет законодателя реагировать на эти изменения[1].

В этой связи целесообразно несколько заглянуть вперед и определить перспективы развития российского уголовного законодательства под углом зрения учета факта использования информационных технологий при конструировании норм Особенной части уголовного права. Это позволит не только адекватно оценить степень и характер общественной опасности деяний, но и более четко установить предмет доказывания по уголовному делу, наметить пути расследования и предупреждения подобных преступлений.

Так, изучение гл. 24 УК РФ («Преступления против общественной безопасности») заставляет задуматься над тем, что ряд преступлений террористической направленности достаточно часто совершается при помощи информационных технологий, более того, использование этих средств способствует распространению данных деяний.

Например, очевидно, что склонение, вербовка или иное вовлечение в совершение преступлений, образующих террористическую деятельность (чч. 1–2 ст. 205.1 УК РФ) с использованием указанных выше технологий увеличивает возможности содействия террористической деятельности по привлечению в ряды террористических организаций новых их членов[2]. Но пока рассматриваемый квалифицирующий признак состава данного преступления не указан в ст. 205.1 УК РФ.

Не учтено в качестве квалифицирующего обстоятельства использование информационных технологий в диспозиции ст. 207 УК РФ («Заведомо ложное сообщение об акте терроризма»).

Думается, применение в данном случае одних лишь социальных сетей может породить панику среди населения, парализовать функционирование различных предприятий и учреждений, работу общественного транспорта, объектов социальной инфраструктуры.

Нет каких-то серьезных возражений и в отношении вывода о том, что призывы к массовым беспорядкам, предусмотренным ч. 1 ст. 212 УК РФ, или участие в них, а равно призывы к насилию над гражданами (ч. 3 ст. 212 УК РФ) имеют большую деструктивную силу, чем обычные призывы, хотя бы из-за их способности оказать воздействие на неопределенно большое число пользователей электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет.

В связи с этим включение в ст.ст. 205.1, 207 и 212 УК РФ квалифицирующего признака – использование электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, на наш взгляд, вполне оправданно.

---

[1] По данным Генеральной прокуратуры Российской Федерации, с 2013 по 2016 гг. число преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий, увеличилось в 6 раз – с 11 тыс. до 66 тыс. (Егоров И. Киберпрокурор // РГ. – 2017. – 25 авг.).

[2] Таран Д. Цифровая оккупация.// Завтра. – 2019. – № 1 ; Емельяненко В. Перезагрузить радикала // РГ. – 2018. – 18 мая.

Существуют резервы и при конструировании норм, включенных в гл. 25 УК РФ («Преступления против здоровья населения и общественной нравственности»). Например, согласно п. «б» ч. 2 ст. 228.1 УК РФ, повышенную ответственность влечет сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных информационно-телекоммуникационных сетей (включая сеть Интернет). Однако аналогичное деяние, совершенное в отношении сильнодействующих и ядовитых веществ (ст. 234 УК РФ), не признается преступлением с отягчающим обстоятельством.

Полагаем, что своим негативным воздействием на людей в немалой степени обязано именно использованию информационных технологий, значительно увеличивающих возможности сбыта этих предметов.

Также можно вести речь о влиянии использования вышеназванных технологий на склонение к потреблению наркотических средств, психотропных веществ или их аналогов (ст. 230 УК РФ). И в этом случае возможности привлечения того же Интернета к обработке сознания, например, молодежи, несовершеннолетних в пользу употребления наркотических средств, психотропных веществ или их аналогов велики[1].

Но если это так, то разумно, чтобы законодатель отреагировал на отмеченные выше обстоятельства следующим образом. Включением в ст. 230 УК РФ нового квалифицирующего признака рассматриваемого преступления – использования при совершении этого преступления электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

Аналогичные аргументы можно высказать и в пользу дополнения ст. 240 УК РФ («Вовлечение в занятие проституцией») указанием на такой же квалифицирующий признак – совершение преступления с использованием названных выше информационных технологий. Очевидно, что использование социальных сетей для вовлечения в занятие проституцией расширяет в немалой степени возможности сутенеров развивать эту разновидность секс-бизнеса. Появление подобного квалифицирующего признака в ст. 240 УК РФ в какой-то мере будет способствовать предупреждению данного антиобщественного явления.

Есть основания полагать, что и некоторые преступления в сфере экономической деятельности получили свое распространение благодаря активному использованию информационных технологий. Вспомним финансовые пирамиды «МММ» Мавроди. Без интенсивной помощи СМИ и сети Интернет вряд ли стало возможным вовлечь в эту аферу миллионы людей. Но что мы видим сейчас? В настоящее время ст. 172.2 УК РФ, устанавливающая ответственность за организацию деятельности по привлечению денежных средств или иного имущества, не содержит среди квалифицирующих признаков этого преступления использование информационных технологий. Думается, это ошибка, которая должна быть исправлена на законодательном уровне.

---

[1] По данным МВД России, только в 2017 г. было заблокировано 21 тыс. сайтов, содержащих информацию о наркотических средствах и их обороте (Только факты // Криминал. – 2018. – № 17).

Нет подобного квалифицирующего признака и в ст. 200.3 УК РФ, предусматривающей ответственность за привлечение денежных средств граждан в нарушение требований законодательства Российской Федерации об участии в долевом строительстве многоквартирных домов и (или) иных объектов недвижимости. Бесспорно, и это преступление получило свое распространение во многом за счет использования информационных технологий. Следовательно, появление такого обстоятельства, усиливающего уголовную ответственность за подобное преступление, было бы целесообразным.

Азаров Артем Сергеевич[1],
специалист по сопровождению и внедрению ООО «БалтИнфоКом»

Гром Георгий Юрьевич[2],
специалист по сопровождению и внедрению ООО «БалтИнфоКом»

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ОПЕРАТИВНО-РАЗЫСКНОЙ ИНФОРМАЦИИ ПРИ ФОРМИРОВАНИИ ДАННЫХ НА ОБЪЕКТ ИССЛЕДОВАНИЯ

Система геоинформационного анализа фактографической информации «Следопыт». Исходными данными для анализа в системе может являться практически любая фактографическая информация, биллинговые данные сотовых, спутниковых и других систем связи, данные треккинговых устройств, журналы доступа к серверам, данные систем контроля доступа.

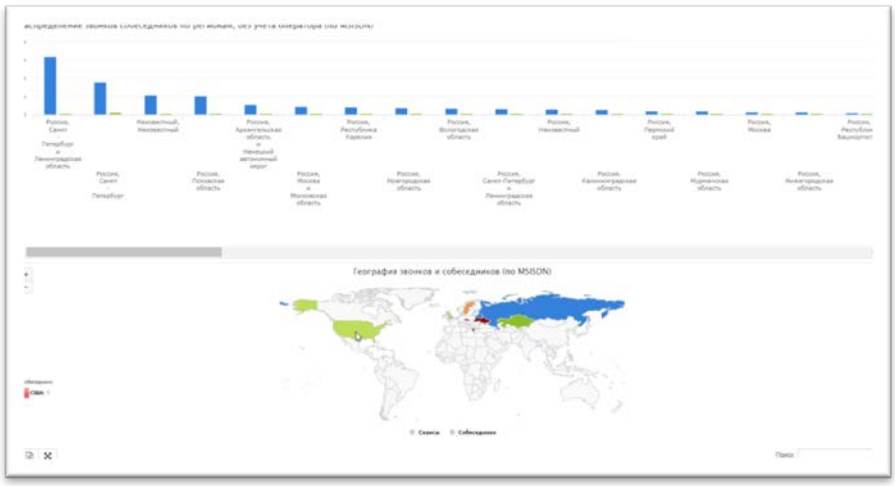

Рис. 1. География собеседников по *MSISDN*

Выведение пользовательских номеров собеседников, терминальных и системных номеров.

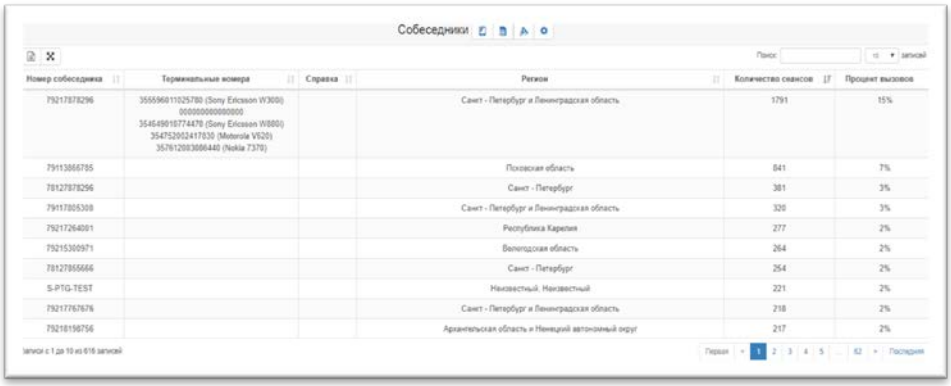

Рис. 2. Анализ собеседников

Функции детализации абонентов инструмент СПО «Следопыт» призван предоставить аналитику возможность сравнить детализации, построенные на

[1] © Азаров А. С., 2019.
[2] © Гром Г. Ю., 2019.

основании загруженных данных и на выборе различных идентификаторов. Функционал этого инструмента очень похож на функционал анализа досье по одному абоненту.

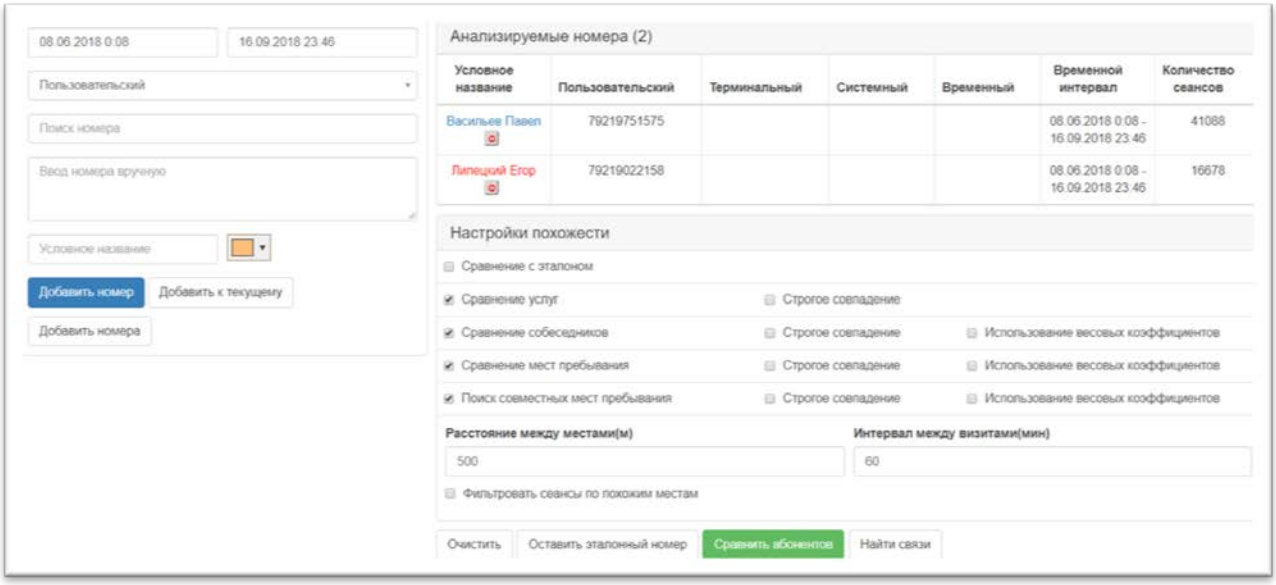

Рис. 3. Выборка стартовых данных

Система интеллектуальной обработки больших массивов информации «Зверобой». Если Следопыт позволяет строить многокритериальные отчеты-досье в случае, если интересующие идентификаторы уже известны, то «Зверобой» – это инструмент для выявления интересующих идентификаторов в условиях высокой неопределенности.

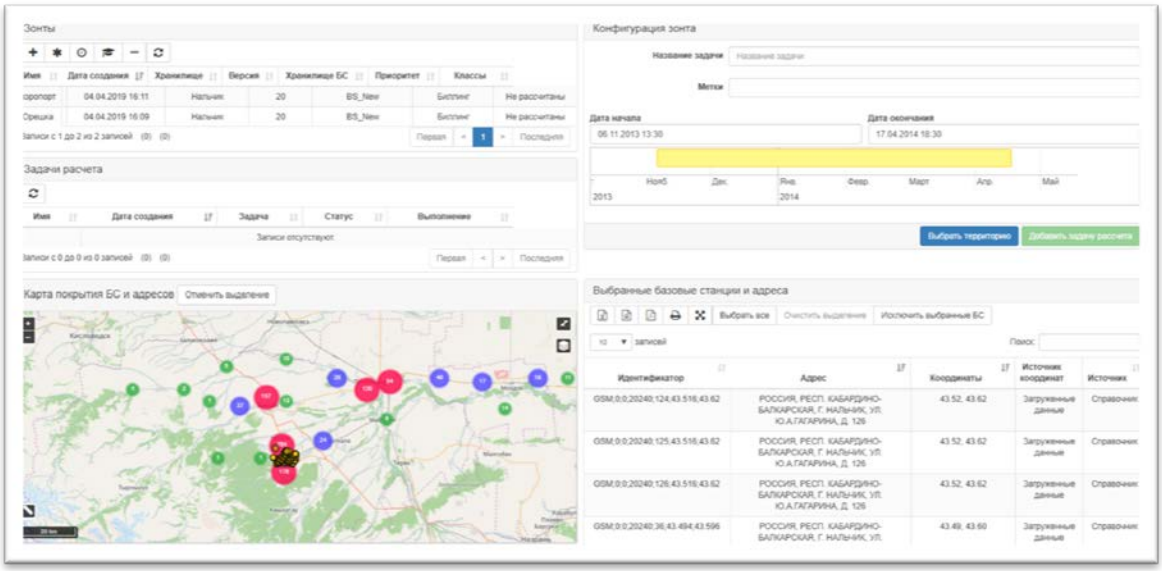

Рис. 4. Анализ разнородной фактографической информации

Существует ряд инструментов для задания различных фильтров, поведенческих шаблонов, поиска скрытых связей между массивами информации, с помощью которых система позволяет сузить массив рассматриваемых идентификаторов с сотен миллионов до десятков – количество, которое поддается дальнейшему подроб-

ному изучению. «Зверобой» работает с теми же структурами данных, что и «Следопыт», системы полностью совместимы.

«Зонты». «Зонт» – это геовременной срез. Иными словами, это массив данных снятых с определенного места за определенное время. Таким образом, мы можем вычленять нужный пласт информации по соответствующим классификаторам из общего массива. По сути, создание зонта позволяет нам снимать все интересующие нас данные за определенный промежуток времени с выбранных БС или иных систем приемо-передачи сигнала.

К данным из зонта можно применять следующие инструменты:

– создавать списки номеров;

– «анализ территории» – построение «Досье абонента» по данным из зонта;

– «ручные запросы» – позволяют выделять из зонтов (с предварительно рассчитанными классификаторами) идентификаторы, удовлетворяющие сложным критериям.

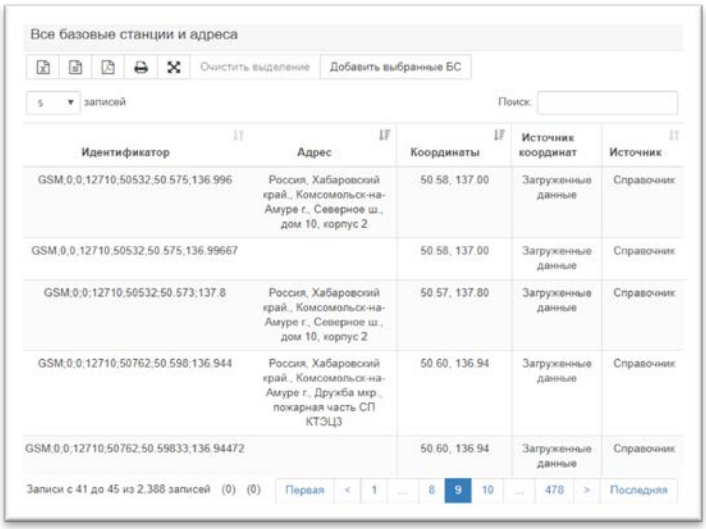

Рис. 5. Создание «зонтов», выбор территории

Система ручной и автоматизированной регистрации, приоритезации и анализа информации о связях сущностей «Октопус». Входящей информацией для системы могут являться справочники, учетные данные, в том числе текстовые, информация, полученная в ходе криминалистического анализа мобильных устройств, автоматически полученная информация из открытых источников – социальных сетей, сайтов знакомств, досок объявлений, порталов резюме и вакансий и др. Также информация может вводиться вручную.

Основным преимуществом системы является ее ориентированность на организацию сведений в базах данных (проектах), имеющих структуру графа. Помимо стандартного полнотекстового поиска, подобная сетевая структура данных в виде графа позволяет применять множество мощных подходов для решения сложных аналитических задач. В первую очередь быстро и удобно осуществлять поиск косвенных и неявных связей и взаимодействий между сущностями различного характера: документами, событиями, местами, лицами, организациями, предметами.

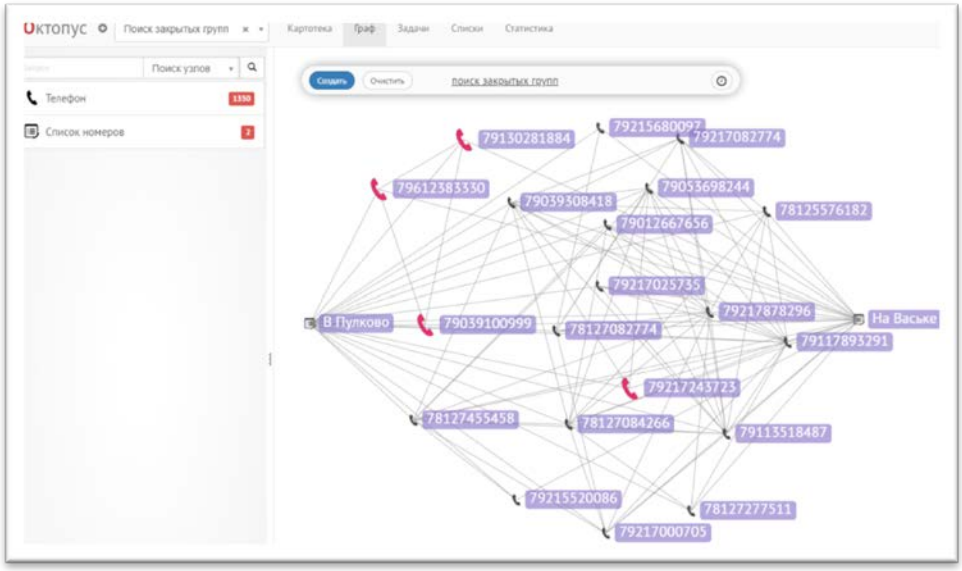

Рис. 6. Визуализация. Построение связей

Гибкость подобного подхода к управлению данными в проектах в сочетании с универсальной низкоуровневой структурой, представленной в формате графа, открывает уникальные возможности для работы с объектами в предметных областях практически любой направленности. Будь то аналитика социальных сетей, новостных и прочих медиа ресурсов сети Интернет или же построение сетей контактов и взаимодействий лиц и организаций на основе оперативных фактографических и учетных данных.

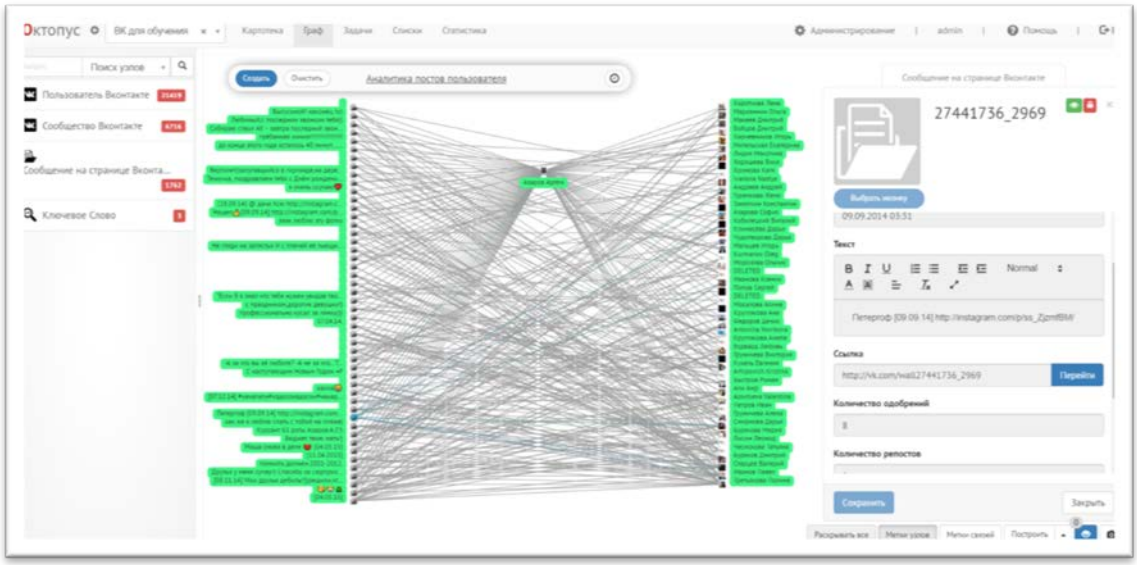

Рис. 7. Анализ постов пользователя на графе

Основные функциональные возможности и сферы возможного применения: структуризация данных в виде графа объектов и связей между ними; составление и организация справочно-аналитических БД (DB); обработка фактографической и учетной информации; аналитика на графах; построение сетей контактов; подключение к ведомственным базам; сбор и обработка данных из открытых источников (госданные, соцсети, новости, объявления); поиск и непрерывный мониторинг сведений из всех подключаемых (сопрягаемых) ресурсов; поста-

новка и запуск задач загрузки данных, как в режиме расписания, так и в режиме онлайн; поиск связей и выявление цепочек связных собеседников; определение пересекающихся контактов; формирование выборки по фильтрам (временным и пр.); создание визуальных отчетов с выделением объектов; построение динамических графов; построение досье; просмотр и изменение свойств объекта; просмотр и добавление связных объектов в табличном представлении; построение аналитических отчетов.

Аксенов Вадим Александрович[1]**,**
старший оперуполномоченный Управления уголовного розыска
УМВД России по Белгородской области

БОРЬБА С КИБЕРПРЕСТУПЛЕНИЯМИ, СОВЕРШЕННЫМИ С ИСПОЛЬЗОВАНИЕМ СЕРВИСОВ IP-ТЕЛЕФОНИИ

Развитие современных информационных технологий, использование последних достижений науки в сфере связи и необходимость обновления информационно-телекоммуникационных систем явились основанием для возникновения нового способа совершения хищений – с использованием средств IP-телефонии.

Так что же представляет собой технология *Voice Internet Protocol*? Суть передачи информации следующая: сигнал переводится из аналогового формата (голос) в цифровой и подается на коммутирующее оборудование, где он зашифровывается и сжимается. В дальнейшем пакет информации по сети Интернет попадает к адресату, где посредством специальных программ и аппаратуры происходит его перекодировка в первоначальный вид. Технология преобразования голоса в цифровой сигнал и его обратное декодирование получило название IP-телефония *VoIP*. Таким образом, посредством сети происходит телефонное общение между абонентами [1].

Данный уровень связи является современным и новым в условиях цифрового развития общества. Технология *VoIP* предоставляет уникальную возможность осуществления звонков по низким тарифам, в связи с чем активно используется в сфере бизнеса. Уже в 2007 г. в Англии, Германии, Франции и США IP-телефония активно использовалась в различных сферах бизнеса и считалась стандартом связи. В Российской Федерации и странах СНГ динамика использования интернет-связи увеличивается с каждым годом [2].

Сервисы IP-телефонии имеют свою классификацию, основной из которых выступает критерий выбора модели протокола:

– **H.323** – предназначен для передачи мультимедийных данных в пакетных сетях. Раньше использовался довольно широко, но сейчас практически вытеснен протоколом SIP. Не связан напрямую с IP-протоколом, однако связь реализуется, чаще всего, с его помощью;

– **MGCP** – протокол контроля медиашлюзов. Используется в распределенных VoIP-системах для передачи голоса по протоколу *IP*;

– **IAX2** – протокол обмена голосовыми данными. В отличие от *SIP* и *H.323*, использует только один порт. Особенность этого протокола – экономия сетевого трафика при обмене данными;

– **SIP** [3].

В данной научной статье мы уделим внимание *SIP* – протоколу, который чаще других используется в качестве средства совершения преступлений данной категории. Считаясь протоколом прикладного уровня, он необходим для производства, изменения и окончания сеансов связи – мультимедийных конференций и телефонных соединений.

---

[1] ©Аксенов В. А., 2019

В качестве основного отличия IP-телефонии от сотовой связи стоит отметить следующее: при осуществлении звонка не требуется привязка к базовой станции сотового оператора и наличие мобильного телефона. В IP-телефонии звонки осуществляются посредством специального приложения (например: *Zoiper*, *MagicApp* и др.), установленного на персональном компьютере или мобильном телефоне через SIP-протокол.

При получении вызова посредством указанного протокола человек видит виртуальный абонентский номер собеседника, т. е. он не имеет сим-карты. Предоставление виртуальных номеров – это услуга IP-провайдеров, осуществляющих работу по принципу переадресации звонков через SIP-протокол.

В 2013 г. русским программистом Павлом Дуровым, основателем социальной сети «ВКонтакте», создан мессенджер *Telegram*. Сервис построен на технологии шифрования переписки *MTProto*. С недавнего времени на базе указанного мессенджера стали появляться так называемые боты, представляющие собой специальные программы, выполняющие автоматически и (или) по заданному расписанию какие-либо действия через интерфейсы [4]. Нас интересуют чат-боты, осуществляющие функции по подмене абонентского номера. В данном случае звонки проходят посредством мессенджера *Telegram* по одному из протоколов IP-телефонии, в результате чего собеседник увидит подменный номер, который может иметь принадлежность к сотовому оператору или IP-провайдеру, в том числе иностранных государств. Как правило, услуги такого рода платные, однако позволяют обеспечить полную анонимность при производстве звонков.

Применение сервиса IP-телефонии позволило преступникам совершать звонки с высокой анонимностью, в том числе за пределами Российской Федерации. При оформлении виртуальных номеров у IP-провайдера не требуется личное посещение офиса, все можно сделать дистанционно посредством электронной почты, в связи с чем предоставляются данные третьих лиц.

Для того, чтобы глубже понять принцип работы сервисов IP-телефонии, давайте обратимся к рассмотрению их базовой составляющей: IP-адрес. Понять, что такое IP-адрес и как он работает первостепенно важно, так как использование сети интернет является краеугольным камнем во многих преступных схемах. IP-адрес – это уникальный идентификационный номер, который присваивается каждому компьютеру при выходе в сеть Интернет. Он представляет собой последовательность из цифр в диапазоне от 0 до 255, чередующихся через точку. Например, 171.208.29.66. IP-адрес присваивается компьютеру его интернет-провайдером в момент начала интернет-сессии: открытия первой страницы, а оканчивается закрытием сессии: последней страницы. Также как и абонентский номер, IP-адрес имеет свой ресурс нумерации, т. е. каждому интернет-провайдеру выделено определенное количество IP-адресов в конкретном диапазоне.

Получение сведений по IP-адресам усложняет использование преступниками легкодоступных средств анонимизации в сети, которые сокращенно называют *VPN* (виртуальная частная сеть). Смысл ее действия заключается в следующем: после подключения к виртуальной частной сети пользователь автоматически подключается к серверу третьего лица, как правило, локализующегося на терри-

тории иного государства. Фактически, запрос на интернет-ресурс проходит аналогичным образом, как было описано ранее, однако в истории соединений сайта остается не реальный IP-адрес пользователя, а IP-адрес использованного им VPN-сервера, который, как показывает практика, в большинстве случаев принадлежит иностранным интернет-провайдерам.

С позиции практической деятельности стоит отметить, что знания в сфере IT-технологий многих преступников далеко выходят за сферу базовых. На постоянной основе используются средства анонимизации, затрудняющие проведение следственных действий и оперативно-разыскных мероприятий. По прогнозам ведущих экспертов в сфере IT-технологий ожидается дальнейший рост преступлений с использованием услуг IP-телефонии, что в свою очередь заметно осложнит оперативную обстановку на территории всей Российской Федерации.

Список литературы

1. Основы, виды, технологии IP-телефонии [Электронный ресурс] // URL: https://www.sviaz-expo.ru/ru/articles/2016/osnovy-vidy-tehnologii-ip-telefonii (дата обращения: 15.11.2019).

2. Днепров А. Г. Бесплатные звонки через интернет. Skype и не только [Электронный ресурс] // URL: https://mybook.ru/author/aleksandr-dneprov/besplatnye-zvonki-cherez-internet-skype-i-ne-tolko (дата обращения 15.11.2019). – СПб. : Питер, 2010.

3. Протоколы IP-телефонии [Электронный ресурс] // URL: http://voiplab.by/wiiki/new-voip-technology/100-protokoly-ip-telefonii (дата обращения: 15.11.2019).

4. Telegram [Электронный ресурс] // URL: https://ru.m.wikipedia.org/wiki/Telegram (дата обращения: 15.11.2019).

Алимова Алина Андреевна[1]***,***
курсант института-факультета
подготовки сотрудников для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]***,***
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В КРЕДИТНЫХ ОРГАНИЗАЦИЯХ

Кредитные организации представляют собой одну из самых важных частей банковской системы любого государства, которая оказывает огромное влияние на жизнь человека и общества в целом, поскольку кредитные организации занимаются обслуживанием производственных нужд и инвестиционных потребностей предприятий, а также являются ключевым элементом расчетного и платежного механизма хозяйственной системы страны. Но с развитием экономики государства преступники также совершенствуют свои противоправные действия в этой сфере.

К наиболее часто встречаемым преступлениям, совершаемым клиентами кредитных организаций, относятся: мошенничество с использованием электронных средств платежа, а также преступления в сфере выдачи и получения кредитов, так как в криминологическом отношении кредитование является одной из самых массовых и уязвимых банковских операций.

Стоит сказать, что правоохранительные органы прикладывают немало усилий для того, чтобы раскрыть данные преступления. При этом существуют определенные сложности, возникающие при проведении дознавателем или следователем какого-либо из следственных действий. Например, таких как выемка, осмотр места происшествия, допрос, обыск, изъятие образцов и наложение ареста. Вместе с тем, анализ складывающейся оперативной обстановки, связанной с IT-преступностью, свидетельствует о наличии ряда проблемных вопросов, препятствующих эффективной организации соответствующих направлений оперативно-служебной деятельности органов внутренних дел и требующих скорейшего разрешения.

Сохраняется возможность у лиц, занимающихся преступной деятельностью, избегать идентификации путем использования программных технологий *VPN, TOR, SSL*, позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров посредством SIP-телефонии.

Применяемые способы шифрования данных на распространенных интернет-сервисах не позволяют устанавливать IP-адреса серверов пользователей, отслеживать их активность, устанавливать данные пользователей. Существующий порядок оформления идентификационных модулей операторами сетей подвиж-

ной радиотелефонной связи порождает комплекс проблем, связанных с установлением абонента в процессе раскрытия преступлений.

До настоящего времени не завершен процесс формирования договорной правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисов, в том числе социальных сетей. Отдельного внимания заслуживает вопрос обеспечения доступа правоохранительных органов к идентификационным сведениям о лицах, совершивших платежные операции посредством банковских и иных платежных систем.

Рассмотрим особенности тактики обыска в кредитных организациях. Согласно положениям ст. 182 УПК РФ, обыск в кредитных организациях – это следственное действие, процесс проведения которого регулируется нормами уголовно-процессуального закона. Данный процесс заключается в обследовании отдельных помещений кредитной организации, а при необходимости и лиц, находящихся в каком-либо помещении. Целью проведения обыска в кредитных организациях является обнаружение и изъятие элементов информационных банковских систем, компьютерной техники, различных носителей компьютерной информации (диски, дискеты, флэш накопители и т. д.), ценностей (ценные бумаги, драгоценные металлы), документов, содержащих сведения о самой кредитной организации и о ее клиентах.

При наличии достаточных данных полагать, что в помещениях, хранилищах определенной кредитной организации, у ее руководителя или у кого-либо из сотрудников находятся средства или орудия совершения преступления, либо имеются предметы, документы, имеющие значение для уголовного дела, органы предварительного расследования производят обыск.

Следователь для того, чтобы реализовать принятое им решение о производстве данного следственного действия, сначала выполняет определенную систему организационных мероприятий, а именно он собирает необходимую ему информацию о кредитной организации, о ее клиентах. В случае необходимости осуществляет подготовку определенных технических и иных средств, необходимых для фиксации самого хода и порядка производства данного следственного действия, после чего занимается определением круга участников обыска, разъясняет им их права и обязанности, которыми они могут пользоваться при производстве данного следственного действия.

В зависимости от характеристик предмета, который будет изыматься, например, это может быть документ, содержащий необходимую информацию, также компьютерная информация или сам компьютер, орган предварительного расследования подготавливает нужные ему средства для упаковки, хранения и перевозки изъятых объектов. К таким средствам можно отнести: электронные носители информации, картонные коробки, белая бумага, полиэтиленовые пакеты, конверты, пластиковые контейнеры, веревка для перевязки и т. д. Также для того, чтобы изъять необходимую для исследования информацию с центрального компьютера органу предварительного расследования нужно подготовить переносную аппаратуру, например, переносные носители, способные вместить

большой объем информации (сменный жесткий диск, дисководы, диски), а также иногда может возникать необходимость в наличии самого переносного компьютера.

Круг участников обыска в кредитной организации определяется в зависимости от того, при каких условиях производится данное следственное действие. К обязательным участникам относятся понятые и представители кредитной организации. Нежелательно привлекать сотрудников кредитной организации в качестве понятых, так как такие понятые фактически могут являться заинтересованными лицами, и результаты производства обыска будут подвергнуты сомнению. В качестве понятых следователь может пригласить лиц, обладающих определенным уровнем знаний о банковских технологиях.

Иногда, при проведении обыска из-за особенностей объектов, имеющих значение для уголовного дела, найти их может только специалист. Поэтому в случае необходимости, например, для получения соответствующих рекомендаций по соблюдению правил техники безопасности при производстве обыска, чтобы не повредить информационные банковские системы, следователь привлекает специалиста. При этом при вскрытии сейфа в кредитной организации участие специалиста обязательно.

Также для наиболее эффективного проведения обыска в кредитной организации могут быть привлечены и сотрудники оперативных подразделений органов внутренних дел.

Обыск в кредитных организациях в основном осуществляется по тем же правилам, что и обыск в жилых и иных помещениях, т. е. на основании судебного решения. Существуют и свои особенности, которые связаны не только с банковской тайной, но и со значительным объемом обыскиваемого пространства, а также невозможностью полностью приостановить деятельность кредитной организации. Органу расследования необходимо учитывать, что различные операции с самими техническими элементами информационных банковских систем могут привести к изменению или уничтожению определенной информации, которая может выступать в качестве доказательств по уголовному делу. Поэтому в первую очередь осматривается центральный управляющий компьютер, на котором хранится наибольшая часть информации. Он также управляет остальными техническими элементами информационной банковской системы. Для того, чтобы предотвратить непосредственный доступ к информации, во время производства следственного действия необходимо отключить вместе с участием специалиста от главного компьютера те элементы информационной банковской системы, которые находятся за пределами помещения, в котором производится обыск.

Как правило, в кредитной организации изымается большое количество элементов информационных банковских систем, для осмотра которых необходимо продолжительное время, поэтому их осмотр может осуществляться не на месте обыска, а по месту производства предварительного расследования. Все изымаемые объекты предъявляются понятым и другим лицам, присутствующим при обыске, упаковываются и опечатываются, что удостоверяется подписями указанных лиц.

По окончании обыска следователь составляет протокол, копия которого под расписку вручается представителю администрации кредитной организации и направляется прокурору.

Следующим следственным действием, особенности которого необходимо рассмотреть, является выемка в кредитной организации. Производство данного действия регулируется нормами уголовно-процессуального закона и заключается в добровольном либо в принудительном изъятии предметов и документов, имеющих значение для уголовного дела. При этом немалую роль играют те обстоятельства, на основании которых можно точно определить, где и у кого эти предметы находятся, так как это является одним из обязательных условий производства выемки. Изыматься могут разные документы, например: выписки по счетам клиентов, переписка, расчетные документы и др.

Органам предварительного расследования необходимо обратить внимание не только на уголовно-процессуальное законодательство, но и на законы, регулирующие деятельность банка, или документы, регламентирующие деятельность той или иной кредитной организации, с целью эффективного производства выемки важных для уголовного дела документов. В зависимости от особенностей деятельности кредитных организаций органы предварительного расследования могут привлекать специалистов, которые благодаря своим специальным знаниям в области банковской деятельности разъясняют следователю возникающие у него вопросы. Само решение о производстве выемки документов в кредитной организации реализуется на основании постановления суда. Данное требование содержится в ст. 183 УПК РФ. Выемка производится следователем принудительно в том случае, если кредитная организация отказывается выдать требуемые документы. Чаще всего бывает так, что сами руководители кредитных организаций препятствуют в выдаче органу предварительного расследования необходимых ему документов, потому что они сами непосредственно причастны к преступлению, совершенному с использованием банковских технологий [1].

Нельзя оставлять без внимания и осмотр изымаемых предметов или документов. Он может осуществляться как на месте проведения выемки, так и производиться как отдельное самостоятельное следственное действие. Это может быть только в случае, если для этого требуется большой промежуток времени, либо необходимо провести какие-либо сложные действия [2].

Наряду с судебным решением, можно выделить еще одну особенность производства выемки в кредитных организациях, к которой относятся определенные проблемы, непосредственно возникающие при производстве выемки. Бывает так, что документы, содержащие информацию о деятельности самой кредитной организации или о ее клиентах, имеют достаточно большой объем, поэтому требуется длительная подготовка для того, чтобы их выдать. В УПК РФ не установлен срок такой подготовки, но в его положениях содержится информация о том, что кредитная организация обязана выдать имеющиеся у нее документы незамедлительно с момента предъявления постановления на производство выемки. Возможно, будет целесообразным внести некоторые дополнения в уголовно-процессуальный закон, которые бы определили данные сроки. Но при этом следует также учитывать и сроки производства предвари-

тельного расследования, которые не зависят от каких-либо объективных трудностей, возникающих при производстве следственного действия.

В ч. 7 ст. 115 УПК РФ предусмотрено такое следственное действие, как наложение ареста на денежные средства и иные ценности, находящиеся на счете, во вкладе или на хранении в банках и иных кредитных организациях. Помимо того, что данное следственное действие ограничивает право собственности, оно также затрагивает и другое не менее важное право, закрепленное в ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», согласно которой кредитная организация, Центральный банк Российской Федерации гарантируют тайну об операциях, счетах и вкладах своих клиентов и корреспондентов [3].

При подготовке к производству такого следственного действия следователь направляет запрос в соответствующую кредитную организацию с целью выяснения, имеется ли у нее в наличии расчетный счет определенного лица. Такой запрос составляется на основании судебного решения и направляется непосредственно руководителю кредитной организации, который обязан предоставить необходимую следователю информацию об этих денежных средствах и иных ценностях. Следователь вправе обращаться к руководителю кредитной организации без соблюдения какой-либо специальной процессуальной формы, так как УПК РФ не содержит в себе сведений о том, в какой форме составляется данный запрос. Также уголовно-процессуальный закон не закрепляет соответствующий объем информации, которую должен предоставить руководитель кредитной организации. Поэтому, если сведения, составляющие банковскую тайну, будут предоставлены в чрезмерном объеме, то это приведет к ущемлению прав не только лиц, в отношении которых необходимо установить данное право ограничение, но и тех лиц, которые не причастны к расследуемому преступлению.

На наш взгляд, в УПК РФ необходимо указать объем той информации об операциях и счетах физических или юридических лиц, которую орган предварительного расследования вправе запрашивать из кредитной организации. А от ответа кредитной организации на запрос будет зависеть содержание постановления о возбуждении перед судом ходатайства о наложении ареста на денежные средства и иные ценности, находящиеся на счете, во вкладе или на хранении в банках и иных кредитных организациях.

Также необходимо ответить на вопрос, связанный с суммой, на которую может налагаться арест. В положениях уголовно-процессуального закона содержится информация лишь о том, что по счету, на который наложен арест, операции прекращаются полностью или частично, но именно в пределах тех денежных средств и иных ценностей, на которые действительно наложен арест. А в положениях постановления Пленума Высшего Арбитражного суда Российской Федерации от 31 октября 1996 г. № 13 говорится о том, что арест налагается не на сами счета ответчика, а только на денежные средства, имеющиеся на его счетах, в пределах заявленной суммы иска. Поэтому операции по данному счету в отношении тех средств, к которым это следственное действие не применялось, не приостанавливаются [4]. В ходе и непосредственно после окончания

производства следователь составляет протокол, в котором указываются, время начала и окончания данного следственного действия [5–8].

Подводя итог, стоит сказать, что проблемы при производстве различных следственных действий в кредитных организациях есть и их надо решать. Ведь с развитием новых технологий преступники также повышают уровень и эффективность выполнения своих преступных действий. А в связи с определенными особенностями проведения таких следственных действий у органа расследования иногда возникают некоторые трудности. Поэтому органу расследования следует учитывать не только требования, предусмотренные УПК РФ, но и требования, предусмотренные режимом реализации банковских технологий, системой функционирования кредитной организации.

Список литературы

1. Постановление Пленума Верховного Суда Российской Федерации от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)».

2. Кульков В. В. Расследование и предупреждение преступлений: Руководство для следователей и дознавателей : практическое пособие / В. В. Кульков, П. В. Ракчеева ; под ред. В. В. Кулькова. – М. : Издательство Юрайт, 2017.

3. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (ст. 26).

4. Постановление Пленума Высшего Арбитражного Суда Российской Федерации от 09 июля 1997 г. № 12 «О внесении изменения в постановление Пленума Высшего Арбитражного Суда Российской Федерации» от 31 октября 1996 г. № 13 «О применении Арбитражного процессуального кодекса Российской Федерации при рассмотрении дел в суде первой инстанции».

5. Гончар В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4. – С. 14–18.

6. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

7. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

8. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Варминский Виктор Игоревич[1],
курсант 3 «Д» курса
института подготовки сотрудников для органов
предварительного расследования,
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2],
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Социальная инженерия – это система приемов и методов воздействия на человеческое сознание путем применения различных приемов из психологии, социологии и бихевиоризма для достижения конкретного необходимого результата.

Социальная инженерия как явление само по себе не ново, оно успешно практикуется людьми в различных областях нашей жизни.

Использование данного направления достаточно широко, начиная от банальных манипуляций с личным окружением отдельно взятого индивида (пускай и не целенаправленно и не структурированно) и заканчивая манипуляциями с широкой массой людей. В данной научной статье хотелось бы рассказать об использовании социальной инженерии в преступных целях, особенностях преступлений с ее использованием и методами профилактики таких преступлений.

Рис. 1. Виктор Люстиг

Целями социальных инженеров как преступных элементов являются нахождение и установление слабых мест психологической составляющей человеческой личности для того, чтобы воспользоваться этими слабостями и получить необходимые персональные данные, согласие на различные действия, а иногда и сотворения определенного рода «психологической ловушки», чтобы сама жертва обратилась к преступнику.

В истории существуют примеры громких и успешных преступлений с использованием социальной инженерии. Для примера возьмем историю Виктора Люстига.

В. Люстиг – известный аферист и мошенник, был довольно подкованным и коммуникабельным человеком, владел 5 языками и был хорошо осведомлен в вопросе документооборота [1].

На протяжении всей жизни он ловко использовал свои мошеннические трюки – причем довольно успешно, сменил 10 псевдонимов. В одних только Соединенных Штатах Америки его арестовали около 50 раз, но каждый раз освобождали из-за недостатка улик [1].

---

[1] © Варминский В. И., 2019.
[2] © Гончар В. В., 2019.

Его самым известным «делом» стала продажа настоящей Эйфелевой башни дважды в 1925 г. Суть его аферы заключалась в том, что на закрытом аукционе он смог под личиной правительственного агента убедить парижского бизнесмена А. Пуассона, что башня продается под снос. Он смог успешно провернуть свою аферу, так как жертва преступления даже не пошла в полицию, узнав об обмане, потому что попросту постеснялась. Данный трюк ему удалось провернуть еще раз, но на этот раз жертва пошла в полицию и обман был своевременно раскрыт [1].

На данном примере мы видим, как ловко злоумышленники уже в начале прошлого столетия использовали приемы из социальной инженерии. Тут была использована схема, при которой мошенник входит в доверие к жертве путем обмана, представившись авторитетной фигурой представителя власти, за короткий срок смог осуществить свой преступный замысел довольно крупных масштабов. Вследствие этого мы можем себе представить, какого охвата может достичь преступность данного типа в современном мире, особенно с использованием последних достижений технологий.

Преступления с использованием социальной инженерии имеют широкий спектр приемов, методов и схем. Опытный преступник может с легкостью завладеть персональными данными человека, не выходя с ним на прямой контакт, и оставаться анонимным при помощи современных технологий. Есть несколько основных методов достижения преступного умысла в этой сфере, такие как:

1. фишинг;
2. телефонный фрикинг;
3. претекстинг;
4. плечевой серфинг;
5. обратная социальная инженерия.

Разберем каждую из этих техник.

Фишинг – это одна из форм интернет-мошенничества, целью который является получение доступа к конфиденциальным данным интернет-пользователя, а именно – логины и пароли. На данный момент является самой популярной схемой социальной инженерии. Крупные утечки информации зачастую происходят именно вследствие использования именно этой схемы: злоумышленник создает так называемую фишинг-рассылку. Одним из наиболее ярких примеров такого рода атак может послужить сообщение, отправленное на электронную почту жертвы, созданное в форме официального обращения от различных представителей банков, пенсионных фондов или различных платежных сервисов. В них обычно говорится об утечке данных или какой-либо поломке в самой базе данных. В данном письме жертве предлагается ввести свои личные данные для «проверки или восстановления» этой информации, обычно в сообщении прикреплена ссылка на сайт, практически точно повторяющая все элементы официального сайта данной организации (банк, платежный сервис) за исключением каких-то незначительных деталей, на которые жертва может не обратить внимания. На таких сайтах предлагается ввести свои персональные данные (логин, пароль, серия и номер паспорта и т. д.). Жертва вводит данные, которые тут же получает злоумышленник и пользуется ими в своих корыстных целях.

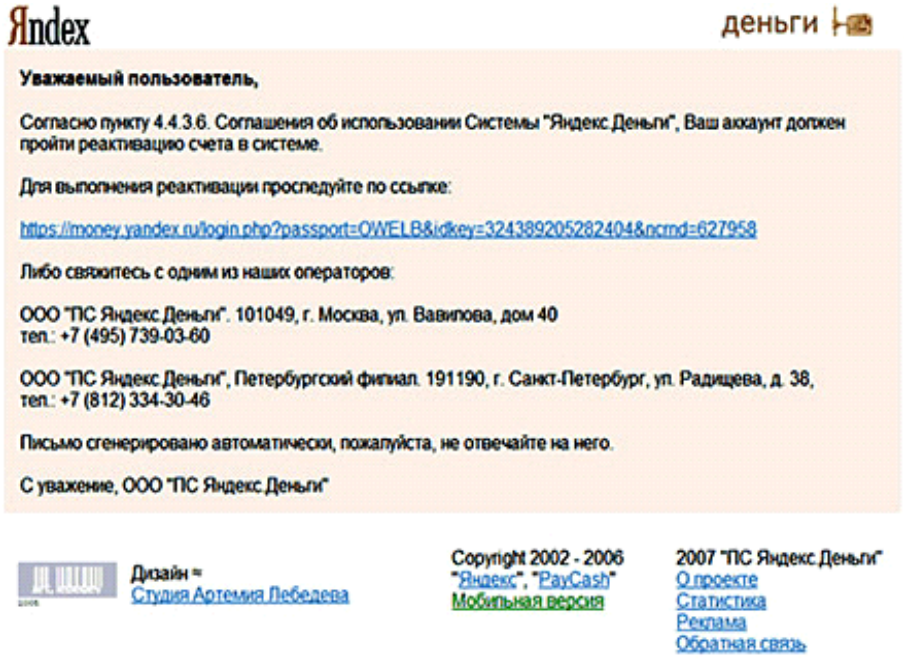

Рис. 2. Пример письма из фишинг-рассылки

Отметим наиболее популярные фишинговые схемы.

Несуществующие ссылки. Смысл данной схемы заключается в том, что на почту жертвы отправляется письмо с провокационным содержанием (например, с требованием обновить данные банковских карт на сервисах, которые используются человеком ежедневно), а переходя по схожей с официальной ссылкой, человек попадает на фальшивый сайт, который практически полностью имитирует содержание официального за исключением небольших неточностей (например. *www.PaypaI.com* вместо *www.PayPal.com* – существует всего лишь одна маленькая неточность: замена буквы *l* на букву *I*; человек вводит свои данные на этом сайте, и они незамедлительно попадают к злоумышленникам).

Подложные лотереи. Внешне это выглядит так: человеку приходит сообщение о том, что он выиграл в лотерее или в каком-либо ином конкурсе, его просят изменить учетные данные какого-либо ресурса для усиления безопасности, и именно в этот момент человек попадает в ловушку.

IVR (телефонный фишинг). Данная техника основана на использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки» банковских и других *IVR*-систем. Обычно жертва получает запрос (чаще всего через фишинг электронной почты) – связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя посредством ввода ПИН-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию. Например, любой может записать типичную команду: «Нажмите единицу, чтобы сменить пароль. Нажмите двойку, чтобы получить ответ оператора» и воспроизвести ее вручную в нужный момент времени, создав впечатление работающей в данный момент системы предварительно записанных голосовых сообщений.

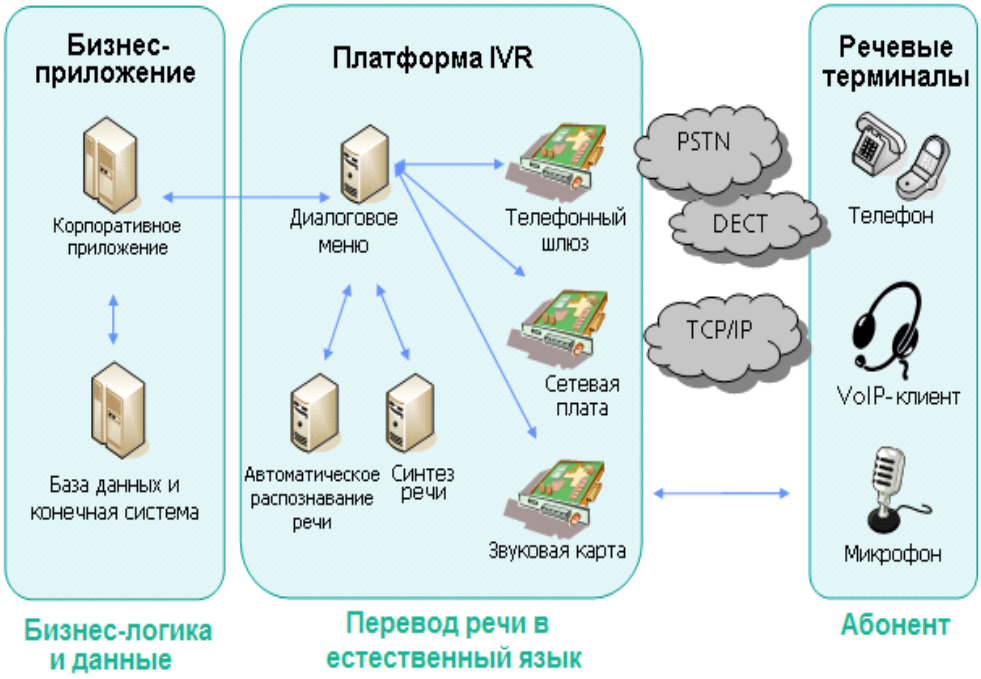

Рис. 3. Схема функционирования телефонного фишинга

Телефонный фрикинг – это термин, который описывает попытки взлома телефонных коммуникаций при помощи манипуляций с тоновым набором. Данная схема появилась в 1950-х годах в США. Телефонная компания *Bell*, которая на тот момент пользовалась большим спросом на предоставление своих услуг и распространялась практически на всей территории страны, прибегала к использованию тонового набора для передачи различных служебных сигналов. Мошенники, которые смогли повторить некоторую часть этих сигналов, получили возможность абсолютно бесплатно звонить и управлять телефонной сетью [2].

Претекстинг – также одна из форм применения преступниками социальной инженерии в современном мире. Данная схема подразумевает представление злоумышленника другим человеком по спланированному сценарию, при помощи которого он получает конфиденциальную информацию о жертве. Данный вид атак подразумевает хорошую подготовку преступника: она состоит в том, что злоумышленник предоставляет якобы правдивую информацию жертве для усыпления ее бдительности. Обычно социальный инженер предоставляет «свои» данные: дату рождения, ИНН, номер паспорта или данные различных счетов. Обычно данный вид мошенничества реализуется по телефону либо с использованием электронной почты.

Также претекстинг имеет две популярные схемы.

«Кви-про-кво» (лат. *qui pro quo* – вместо другого). Смысл данной схемы заключается в том, что злоумышленник обращается в какую-либо компанию, представляется сотрудником технической поддержки и говорит, что обнаружил какую-либо проблему на рабочем месте жертвы. Далее, когда он понимает, что жертва ему поверила, он приступает к «решению» данных проблем, в процессе заставляя жертву совершать действия, позволяющие провести успешную атаку или установить вредоносное программное обеспечение.

«Дорожное яблоко» – в данной схеме злоумышленник подбрасывает зараженный физический носитель данных (например, флеш-карту, *SSD*-накопитель и т. д.) в общественных местах, где его могут легко найти. Носитель оформляется в соответствии с компанией, которую хотят атаковать. Например, подбрасывается флеш-карта, на которой изображен логотип компании. После нахождения – из любопытства – какой-либо сотрудник вставляет найденную флеш-карту в свой компьютер и заражает его вредоносным ПО.

Плечевой серфинг – это тип атаки, при котором идет наблюдение за личной информацией жертвы непосредственно в реальной жизни. Данная форма распространена в людных местах: вокзалах, аэропортах, торговых центрах. Плечевой серфинг происходит в момент ввода жертвой своих персональных данных при оплате каких-либо услуг или регистрации в местах, где требуется непосредственный ввод этих данных. Злоумышленник просто смотрит на человека, который вводит свои данные, запоминает, а позже распоряжается ими.

Обратная социальная инженерия – пожалуй, самый «идеальный» вид использования социальной инженерии, так как жертва даже не понимает, что сама лично отдает именно злоумышленнику все необходимые данные, соответственно, процесс поимки злоумышленника заметно усложняется. Суть данной формы мошенничества заключается в том, что преступник работает непосредственно вместе с жертвой: он умышленно портит какие-либо данные на ее компьютере, после чего жертва замечает это, и злоумышленник говорит о том, что может исправить ее проблему. Зачастую жертва в силу человеческих факторов или перед страхом не справиться с работой просит преступника исправить эту проблему. Преступник соглашается помочь человеку, затем объявляет, что для ускорения решения поставленной «задачи» ему нужны персональные данные, после чего жертва спокойно отдает ему всю необходимую информацию. Особенность данного вида атак заключается в том, что после успешной кражи данных со всеми вытекающими последствиями доверие жертвы к преступнику только усиливается, так как он якобы помог решить ей проблему; возможно, в дальнейшем коллеги жертвы будут обращаться за «помощью» к данному злоумышленнику.

Теперь хотелось бы рассказать о проблеме преступности с использованием социальной инженерии в современной России. Данная проблема стоит особенно остро, так как преступления в этой сфере стали пользоваться пугающей популярностью [3]. В основном успех этих преступлений зависит от нескольких параметров:

1. Низкая киберграмотность.

Приведем статистику Центрального банка Российской Федерации. ЦБ РФ отмечает определенный перечень рисков, с которыми сталкивается рядовой пользователь мобильных устройств:

а) низкая осведомленность и техника информационной безопасности – 29 %;
б) потеря гаджета – 27 %;
в) кража мобильных устройств – 11 %.

Исходя из этих данных, мы можем наблюдать уникальную ситуацию, сложившуюся в России по сравнению с другими странами, где преступления с использованием социальной инженерии по телефону имеют не такую сильную

популярность. «Цифра 29 % говорит, к сожалению, о том, что наши граждане иногда недооценивают риски, которые они должны учитывать при работе с цифровыми инструментами, – сказала первый заместитель председателя ЦБ РФ О. Скоробогатова. – Эта неосведомленность или неосторожность приводит к тому, что у нас очень часто происходит утечка информации именно по этой причине. Иногда люди передают свои пароли, не понимая, что они тем самым передают данные о себе и доступ к своему счету».

Примерно в ⅓ случаев люди лишаются средств на своем счету ввиду своей собственной невнимательности [4–7], чем преступники с успехом пользуются.

2. Утечка баз данных из государственных структур и коммерческих организаций.

Центральный банк Российской Федерации считает, что второй по важности причиной, по которой социальная инженерия в России настолько эффективна, является утечка баз данных. «В большинстве случаев злоумышленники используют информацию, собранную из открытых источников, а также благодаря утечкам баз данных из госструктур и коммерческих организаций», – рассказал руководитель аналитического центра *Zecurion* В. Ульянов.

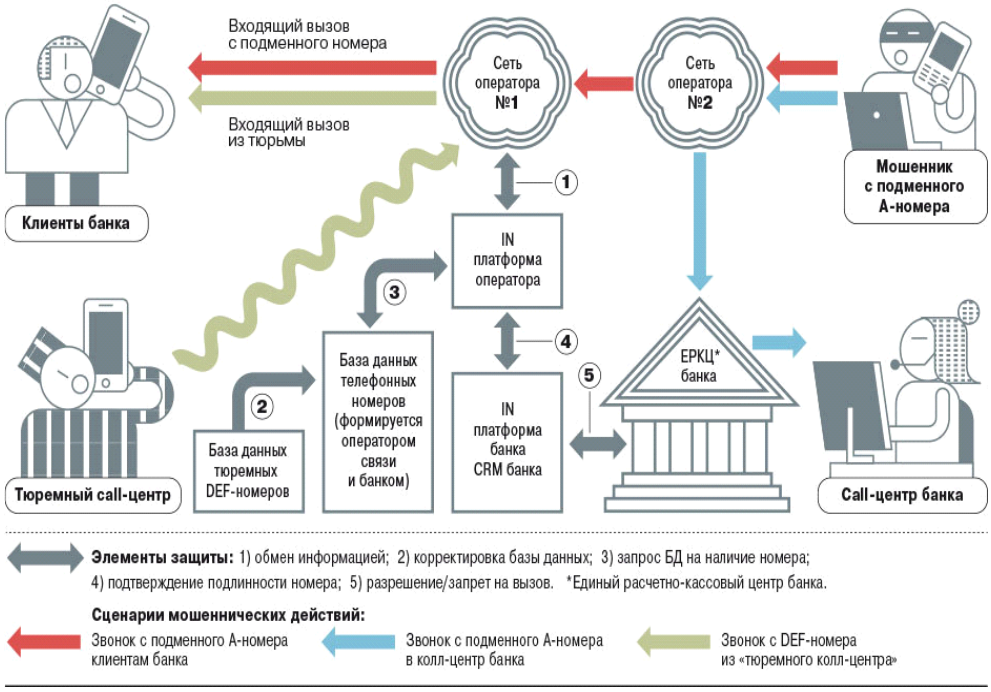

Рис. 4. Схема борьбы с социальной инженерией

В своей презентации Центральный банк Российской Федерации указал на 2 главных источника утечки информации:

1) банки и финансовые организации – 25 %;
2) государственные и силовые структуры – 18,8 %.

На сегодняшний день опасность данных преступлений заключается в их открытом характере. Существует ряд форумов, на которых мошенники продают персональные данные. В данном преступном сообществе создалась хорошая система коммуникации и администрирования. Люди активно интересуются данными форумами, на данных интернет-порталах создана налаженная инфраструктура, в которой

существет система рейтинга для «проверенных» торговцев конфиденциальной информацией.

Из данных государственных и силовых структур следует, что наиболее часто происходит отток данных из баз: «Магистраль», «Сирена», «Граница», «Мигрант», «Кронос», «Спарк», «Поток», комплексных баз ИБДР-ИБДФ. Несмотря на эти сведения, приоритетными для социальных инженеров являются базы данных из банков.

«Если мы посмотрим на ближайшие два года, как эксперты оценивают технологии, которые, с точки зрения информационной безопасности, наиболее будут подвержены атакам или попытке атак на них, то это большие данные (*Big Data*) – 70 %, – сказала О. Скоробогатова. – Данные – это новая нефть, данные – фактически новая бизнес-модель, новая возможность создавать продукты и услуги. Обладая большими данными, мы имеем уязвимость, если базы данных не защищены».

Подводя итоги работы, хотелось бы сказать, что основная причина, по которой преступления с использованием социальной инженерии в современном мире имеют такую популярность и успех – банальный «человеческий фактор». Противостоять этой преступности в современных условиях действительно трудно, но в интересах обеспечения информационной безопасности в современной действительности нужно сделать приоритетной задачей именно профилактику и предупреждение данных преступлений путем работы с населением, доведения необходимой информации и оперативной работы государственных органов. Если говорить конкретнее, то необходимо массовое внедрение информации о том, как обезопасить себя от атак социальных инженеров. Также стоит сказать о том, что необходимо совершенствовать работу органов государственной власти, повышать квалификацию сотрудников органов безопасности государства введением в программу подготовки кадров дисциплин, которые будут освещать данные вопросы, и, конечно, совершенствовать технологическую составляющую в сфере информационной безопасности.

Список литературы

1. Люстиг Виктор [Электронный ресурс] // Википедия. URL: https://ru.wikipedia.org/wiki/Люстиг_Виктор.

2. Информационный портал Habr [Электронный ресурс] // URL: https://habr.com/ru/news/t/459278.

3. Сбербанк предупредил о мошенниках, применяющих социальную инженерию [Электронный ресурс] // URL: https://ria.ru/20190619/1555705485.html (дата обращения: 19.06.2019).

4. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

5. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельно-

сти: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

6. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

7. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Гончар Владимир Владимирович[1]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В НАСТОЯЩЕЕ ВРЕМЯ

В настоящее время прослеживается тенденция увеличения числа задокументированных киберпреступлений, что обусловлено активизацией работы правоохранительных органов по совершенствованию законодательной и нормативной базы, позволяющей выстраивать наиболее эффективные алгоритмы их выявления, раскрытия.

Так, в последние годы приняты:

– Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», которым введены дополнительные составы: «Кража с банковского счета, а равно электронных денежных средств» и «Мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств», относящиеся к категории IT-преступлений;

– Федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», которым было усилено противодействие хищению денежных средств, запущены автоматизированные системы «ФинЦЕРТ» и «Фид-Антифрод», а также кредитно-финансовые организации наделены полномочиями своевременно блокировать незаконные транзакции.

Кроме того, разрабатываются:

– проект федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации», наделяющий Банк России правом досудебной (внесудебной) блокировки фишинговых сайтов и мошеннических колл-центров, что в сочетании с выполнением кредитно-финансовыми организациями требований действующего законодательства в области обеспечения информационной безопасности призвано обеспечить комплексную защиту средств клиентов;

– проект федерального закона «О внесении изменений в Федеральный закон «О банках и банковской деятельности», в соответствии с которым предлагается сократить сроки предоставления правоохранительным органам запрашиваемой информации до 10 рабочих дней;

– проект федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия финансированию терроризма и иных противоправных деяний», включающий, в частности, внесение в Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» статьи, предусматривающей введение внесудебного механизма блокировки банковских счетов (вкладов) и электрон-

[1] © Гончар В. В., 2019

ных средств платежа, при наличии достаточных оснований по их использованию в целях незаконного оборота наркотических средств, психотропных веществ, их аналогов или прекурсоров;

– проект федерального закона «О цифровых финансовых активах», которым предусмотрен механизм регулирования оборота криптовалюты, основанный на стандартах Группы разработки финансовых мер борьбы с отмыванием денег, направленный на снижение привлекательности ее использования в противоправных целях.

Важной особенностью киберпреступлений является их межрегиональный характер, что требует значительных временных затрат на подготовку и проведение необходимых оперативно-разыскных мероприятий по их документированию и раскрытию.

В МВД России осуществляются активный поиск и внедрение в практическую деятельность новых форм и методов противодействия киберпреступлениям. Организовано взаимодействие с Роскомнадзором, Генеральной прокуратурой Российской Федерации, интернет-провайдерами.

Большое значение придается профилактике киберпреступлений, в том числе путем информирования населения с помощью СМИ о новых способах их совершения [1].

Анализ статистики киберпреступлений в 2019 г. свидетельствует о наличии ряда проблемных вопросов, препятствующих эффективной организации соответствующих направлений оперативно-служебной деятельности органов внутренних дел и требующих скорейшего разрешения.

Преступники нередко продолжают избегать идентификации путем использования программных технологий *VPN, TOR, SSL,* позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров посредством SIP-телефонии [2].

Использование программ «анонимайзеров» на распространенных интернет-сервисах не позволяет устанавливать IP-адреса серверов пользователей, отслеживать их активность, устанавливать данные пользователей. Существующий порядок оформления идентификационных модулей операторами сетей подвижной радиотелефонной связи порождает комплекс проблем, связанных с установлением абонента в процессе раскрытия преступлений.

В настоящее время не завершен процесс формирования договорной правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисами, в том числе с социальными сетями.

Кроме того, нередки случаи неисполнения коммерческими организациями запросов, направленных оперативными подразделениями органов внутренних дел, а также согласования перечня сведений, представляющих интерес для получения в рамках межведомственного взаимодействия.

До конца не сформированы эффективные механизмы взаимодействия органов внутренних дел с заинтересованными ведомствами и коммерческими орга-

низациями, предусматривающие возможность оперативной блокировки сайтов интернет-пирамид (хайп-проектов), фишинговых сайтов и мошеннических колл-центров, а также номеров телефонов, с использованием которых осуществляются мошеннические действия.

Операторами сотовой связи, IP-телефонии, интернет-провайдерами не в полной мере выполняются требования постановления Правительства Российской Федерации от 12 апреля 2018 г. № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» по срокам хранения информации в течение 6 месяцев с даты окончания их приема, передачи, доставки и (или) обработки.

В настоящее время еще формируется механизм блокирования вредоносного программного обеспечения для операционных систем мобильных устройств, используемого в целях хищения денежных средств со счетов через услугу «Мобильный банк».

Кроме того, существует острая необходимость в рамках единой базы данных «Дистанционное мошенничество» информации о зарегистрированных киберпреступлениях, а также создания автоматизированных систем мониторинга сети Интернет, в частности, информационных систем поиска по метаданным [3].

Изучение складывающейся правоприменительной практики свидетельствует о важности продолжения работы по дальнейшему совершенствованию имеющейся нормативной базы, организации практической работы правоохранительных структур по выявлению, раскрытию и расследованию киберпреступлений, в том числе путем внесения изменений и дополнений в отдельные положения Уголовного кодекса Российской Федерации, Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» и Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи». Не устранены пробелы в правовой регламентации механизма ареста виртуальных активов в целях их конфискации.

Существует неопределенность при квалификации хищений по п. «г» ч. 3 ст. 158 УК РФ и п. «в» ч. 3 ст. 159.6 УК РФ. Несмотря на разъяснения, изложенные в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в данных нормах не учитывается конкретный способ хищения денежных средств с банковских счетов, что в свою очередь вызывает различия в трактовке со стороны следствия, органов прокуратуры и суда.

Не урегулированы вопросы организации взаимодействия следователей, дознавателей и сотрудников оперативных подразделений территориальных органов МВД России, осуществляющих расследование и раскрытие IT-преступлений, а также активизации сотрудничества с правоохранительными органами иностранных государств.

С учетом вышеназванного киберпреступления позволительно выделить как самостоятельную обособленную разновидность противоправных деяний, кото-

рую отличает собственная специфика в способах их подготовки, совершения и сокрытия.

Один из первоочередных вопросов, требующих решения, это совершенствование кадровой политики и организации подготовки для органов внутренних дел специалистов в сфере противодействия киберпреступлениям.

Необходимы срочные меры, направленные на совершенствование методов информирования населения, в том числе с привлечением федеральных и региональных СМИ, а также социальных медиа, о способах совершения киберпреступлений, методах защиты от них, а также заимствование положительного опыта правоохранительных органов иностранных государств по созданию и распространению в свободном доступе мобильных приложений для смартфонов, позволяющих блокировать входящие вызовы, осуществляемые с номеров телефонов, внесенных в «черный список» как потенциально используемых при осуществлении мошеннических действий [4].

Список литературы

1. Ермаков С. В. Проверка сообщений о преступлениях экономической направленности: пути совершенствования законодательства // Научный портал МВД России. – 2017. – № 2 (38). – С. 25–29.

2. Есина А. С. Об эффективности использования криминалистических полигонов в процессе обучения курсантов и слушателей Института подготовки сотрудников для органов предварительного расследования // Практическая направленность обучения как форма интегрированной подготовки специалистов для органов предварительного расследования Сборник научных трудов Всероссийской научно-практической конференции. – 2017. – С. 5–9.

3. Макеева Н. В. Проведение практических занятий по дисциплине «Расследование преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ» с использованием полигонной базы // Практическая направленность обучения как форма интегрированной подготовки специалистов для органов предварительного расследования : сборник научных трудов Всероссийской научно-практической конференции. – 2017. – С. 42–46.

4. Якупов Р. Х. Особенности расследования преступлений с участием иностранных граждан / Р. Х. Якупов, А. А. Орлова, Е. А. Степанов. – М., 1994. – С. 54.

5. Аналитические материалы МВД России за 2019 год.

Данилова Юлия Викторовна[1]*,*
курсант 3 «Д» курса института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]*,*
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ДЕЯТЕЛЬНОСТЬ СЛЕДОВАТЕЛЯ ПО РАССЛЕДОВАНИЮ КРАЖ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ ИЛИ КРАЖ С БАНКОВСКОГО СЧЕТА

В настоящее время становится актуальной проблема расследования краж денежных средств граждан с электронных носителей или с банковского счета. Для этого киберпреступники используют различные ресурсы, начиная от вредоносных компьютерных программ, банковских технологий, заканчивая троянскими программами-шпионами, которые воруют деньги из электронных кошельков пользователей, например, со счетов пользователя в *WebMoney*, *PayPal*, *QIWI* или «Яндекс.Деньги». Платежные средства, которые существуют только в электронном виде, в основном используются в сети Интернет. Целью написания данной статьи является изучение вопросов, возникающих у следователей органов внутренних дел по уголовным делам данной категории. Попробуем проанализировать основные проблемы, которые влияют на результативность предварительного расследования.

Электронные денежные средства – это безналичные средства в рублях или иностранной валюте, которые учитываются кредитными организациями без открытия банковского счета и переводятся с использованием электронных платежных средств в соответствии с Федеральным законом от 27 июня 2011 г. №161-ФЗ «О национальной платежной системе». Они используются при осуществлении безналичных расчетов. Оказывать услуги по переводу электронных денежных средств в соответствии с законодательством Российской Федерации вправе только кредитные организации, которые уведомили Банк России о начале осуществления определенной деятельности. Другими словами – это средства, которые передаются от одного лица к другому без открытия банковского счета, а также с распоряжением перечислить эти деньги третьим лицам.

Банковский счет – это счет физических и юридических лиц, открытый и поддерживаемый в банке, на котором отражается движение их денежных средств. Банковские счета являются способом учета преступлений и изъятий денежных средств каждым клиентом банка, а также на них отражаются финансовые операции клиентов. Он имеет 20-значное обозначение и к нему привязана одна или несколько банковских карт с определенным идентификационным 16-значным номером. Таким образом, высокие темпы развития современных информационных, финансовых, банковских и кредитных технологий дают возможность пре-

ступникам с помощью новых платежных механизмов получать доход при самых минимальных затратах и рисках быть привлеченными к уголовной ответственности [1].

Ужесточена санкция ст. 159.3 УК РФ, которая предполагает ответственность за мошенничество с использованием электронных платежных средств. Приведенные составы преступления отличаются способом и методом совершения преступления. Пункт «г» ч. 3 ст. 158 УК РФ предусматривает ответственность за тайное хищение денежных средств с банковского счета или электронных денежных средств. Например, лицо тайно похитило банковскую карту с ПИН-кодом, далее использовало устройство самообслуживания и с его помощью произвело снятие денег с банковского счета потерпевшего.

В соответствии с разъяснениями постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в случае, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты, преступление квалифицируется, как мошенничество [2].

Расследованием по уголовным делам о кражах электронных денежных средств или краж с банковских счетов с помощью использования вредоносных компьютерных программ являются установление всех данных о совершенном преступлении, сбор необходимой информации и доказательств виновности конкретных лиц.

Если проанализировать судебно-следственную практику, то можно заметить, что расследование киберпреступлений представляет особую сложность [3–6]. Их особенность в многоэпизодности противоправной деятельности, разном характере периода совершения преступлений, частом затруднении в вопросах сотрудничества свидетелей и задержанных. Стоит отметить нежелание людей обращаться в правоохранительные органы за помощью, так как существуют различные методы совершения подобного рода преступлений. К примеру, злоумышленники могут за короткий промежуток времени обработать большое количество банковских карт, снимая при этом небольшие суммы денежных средств. В результате у следователей возникают трудности в работе с большим объемом процессуальных действий и оперативно-розыскных мероприятий.

Противодействие расследованию киберпреступлений, совершающихся с помощью банковских и иных технологий, понимается как совокупность различных неправомерных действий (бездействий) участников уголовного процесса в отношении фактических данных, имеющих криминалистическую значимость. Представленные деяния совершаются с помощью взаимодополняющих друг друга действий кредитных организаций и Банка России. Они обеспечены всеми необходимыми ресурсами. Эти ресурсы, в свою очередь, направлены на систематическую и комплексную реализацию банковских операций для того, чтобы воспрепятствовать предварительному расследованию [7].

Проводя анализ и оценку информации по данной теме, мы обнаружили определенную статистику в исследовании В. В. Лысенко. Для изучения преступлений, которые совершаются с использованием банковских, кредитных и иных технологий была запрошена оперативная информация у 80 органов предварительного расследования в системе ОВД за 2015–2017 гг. Были опрошены 420 следователей и изучены порядка 120 уголовных дел рассматриваемой категории. Полученные данные были проанализированы и обобщены. Был сделан вывод о том, что киберпреступления, в том числе кражи электронных денежных средств на практике квалифицируются по ст.ст. 159–159.6, 172, 176, 183, 195–197, 272, 273 УК РФ. Наиболее часто данные преступления совершаются при помощи кассовых и расчетных операций, а инструментом банковской деятельности выступают расчетные и кредитные банковские карты.

Следует отметить, что ст. 159.6 УК РФ появилась не так давно. Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» УК РФ был дополнен данной статьей. В соответствии с новой нормой за хищения денежных средств и иного имущества посредствам ввода, удаления, блокирования компьютерной информации, иного вмешательства в функционирование средств хранения предусмотрена уголовная ответственность, которая должна защитить отношения собственности, имущественные интересы, охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей.

На основании данных официальной статистики можно сделать вывод о том, что, несмотря на появление данной статьи УК РФ, ее редко применяют правоохранительные органы. При расследовании уголовных дел данной категории выявляются ошибки и недочеты, в результате чего они не доходят до судебного разбирательства.

Данные следственной практики показывают, что такие преступления, как хищения денежных средств с банковского счета, квалифицируются по п. «г» ч. 3 ст. 158 «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств», ст. 159 «Мошенничество», ст. 159.3 «Мошенничество с использованием платежных карт» и по ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Деятельность сотрудников правоохранительных органов по указанным выше делам часто не эффективна из-за нехватки у следователей необходимых знаний и умений о вредоносных компьютерных программах и имеющихся научно-технических достижений в этой области. Были проанализированы работы Е. С. Шевченко, который в своем исследовании провел опрос среди следователей (респондентами стали 185 следователей и 25 дознавателей). После обобщения данных был сделан вывод о том, что 95 % имеют юридическое образование и лишь 5 % опрошенных получили дополнительную специальную подготовку (образование по специальности «информатика и вычислительная техника»). 60 % сотрудников оценивают уровень владения персональным компьютером как «среднестатистический пользователь», 40 % – как «продвинутый». Около 80 % опрошенных следователей получают необходимые знания в области ком-

пьютерных технологий самостоятельно, т. е. занимаясь самообразованием, 20 % – с помощью курсов повышения квалификации для сотрудников правоохранительных органов, а 5 % – с помощью платных коммерческих курсов или специального образования. Таким образом, из вышеприведенной статистики можно сделать вывод о слабой подготовке следователей и дознавателей ОВД в области компьютерных и информационных технологий.

Подводя итоги данной научной статьи, хотелось бы сказать о необходимости повышать квалификацию сотрудников правоохранительных органов в данной сфере. Необходимо в первую очередь работать на предупреждение данных преступлений, так как они очень сильно подрывают материальное состояние граждан. Несмотря на постоянное совершенствование систем информационной безопасности самих банковских организаций, правоохранительным органам нужно перенимать опыт гражданских экспертов в области информационной безопасности. Также имеются основания полагать, что данный вид преступности стремительными темпами перерастает в международный. Именно поэтому необходимо наладить методику взаимодействия с другими государствами в этой сфере для успешной борьбы с данным видом преступлений.

В заключение хочется отметить, что сейчас киберпреступлениям в нашей стране стало уделяться больше внимания. Так, глава Министерства внутренних дел Российской Федерации генерал полиции В. А. Колокольцев после подведения итогов заседания коллегии принял решение о создании в системе Министерства подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологий. Об этом рассказал официальный представитель МВД России И. Волк. По ее словам, новые подразделения сформируют без увеличения штатной численности ведомства [8].

Список литературы

1. Информационное письмо Банка России от 11.03.2016 № ИН-017-45/12 Памятка «Об электронных денежных средствах».

2. Генеральная прокуратура Российской Федерации [Электронный ресурс] // URL: https://procrf.ru/region/1-generalnaya-prokuratura-rf.html.

3. Мешков М. В., Гончар В. В. Досудебное соглашение о сотрудничестве: проблемы и перспективы // Закон и право. – 2011. – № 1. – С. 92–94.

4. Предварительное следствие в органах внутренних дел / под ред. М. В. Мешкова. – 2-е изд., перераб. и доп. – М., 2007.

5. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

6. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

7. Федеральный закон от 27 июля 2011 г. № 161-ФЗ (ред. от 02.08.2019) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 15.09.2019).

Козлова Наталья Сергеевна[1]*,*
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]*,*
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОБЩАЯ ХАРАКТЕРИСТИКА РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Наша страна на данном этапе своего развития находится на пути к постиндустриальному типу общества. Это обусловлено тем, что такой ресурс как информация начинает постепенно проникать во все сферы общественной жизни, в том числе в экономику. Постепенно на базу информационных технологий осуществляют переход каждый из элементов экономической деятельности: производство, распределение, обмен и потребление. Особенно заметной для граждан является информатизация сферы денежного обращения, на это указывает все более и более возрастающий интерес к безналичным средствам платежа, в том числе к электронным деньгам.

Первая в России электронная платежная система *CyberPlat* начала функционировать в 1997 г. Система электронных денег получила в нашей стране мощный импульс развития, и уже в 2009 г. каждым 15-м жителем России был открыт интернет-кошелек [1]. Тогда же была создана Ассоциация участников рынка электронных денег, которая активно включилась в деятельность законодательных органов по нормативно-правовой регламентации данной сферы общественной жизни. Результатом данной совместной деятельности стало принятие в 2011 г. Федерального закона № 161-ФЗ «О национальной платежной системе», впервые официально закрепившего понятие электронных денежных средств, единые требования к операторам электронных денежных средств (исключительно кредитные организации, имеющие лицензию Центрального банка Российской Федерации), виды электронных кошельков и др.

В соответствии с данным законом, электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа). Иными словами, суть электронных денег заключается в том, что клиент предоставляет фиатные деньги оператору электронных денежных средств, он их учитывает и по распоряжению клиента передает их по назначению за товары, услуги, либо

другим людям. Причем в отличие от безналичных денег, реализуемых с помощью банковских карт, хранение и перевод электронных денег осуществляется с помощью не банковского счета, а виртуального – электронного кошелька, создаваемого путем регистрации учетной записи на ресурсе электронной платежной системы [2].

Согласно статистическим данным Центрального банка Российской Федерации, прослеживается ежегодный рост пользователей электронных платежных систем. Так, в 2018 г. электронными платежными системами в России пользовались более 10 млн человек, было совершено более 2 млрд операций на общую сумму около 1,7 трлн рублей [3].

Такая популярность расчетов электронными деньгами обусловлена рядом их преимуществ: высокой скоростью расчетов (они поступают на счет получателя практически мгновенно, что значительно ускоряет обменные процессы, а это крайне необходимо при современном темпе жизни и в реалиях современного экономического развития, проходящего в условиях глобализации), простотой получения электронного кошелька и анонимностью.

Вместе с тем, данные преимущества послужили благоприятной средой для усложнения существующей преступной деятельности, а также к появлению новых общественно опасных деяний. С использованием электронных денежных средств в интернет-пространстве протекают незаконный оборот наркотиков, оружия, проводятся незаконные азартные игры, финансируется терроризм и подпольный рынок киберпреступности, осуществляется отмывание денежных средств, добытых преступным путем их обналичивания. Растет количество таких новых преступных деяний, как фишинг (пользователь самостоятельно вводит свои данные на сайте, созданном мошенником), его разновидности: вишинг (через звонок) и смишинг (через смс-сообщения), фарминг (скрытое перенаправление потенциальных жертв мошенничества на ложные IP-адреса в сети Интернет). Нередки случаи получения злоумышленниками по поддельной доверенности дубликатов сим-карт, к которым привязаны электронные кошельки. Также нередко используется пиратский софт, посредством которого телефон или компьютер пользователя заражается вирусом, передающим злоумышленникам все данные, которые пользователь вводит в своем интернет-браузере.

Активное перетекание преступности в информационную сферу неизбежно, данный процесс является издержкой повсеместной информатизации. Информацию о методиках хищений, о том, как писать вирусы, как ими пользоваться, как взламывать сайты можно найти в открытом доступе в Интернете. Сами же вирусы являются распространенным товаром на торговых площадках Даркнета (*DarkNet*). При этом уровень киберграмотности и цифровой гигиены основной массы населения нашей страны оставляет желать лучшего.

Такое положение дел простимулировало государственную политику к проведению агрессивных превентивных реформ в отношении электронных платежных систем.

Так, с 15 сентября 2019 г. перед совершением любых транзакций с web-кошелька пользователь должен пройти идентификацию личности на портале Госуслуг (указать данные российского паспорта и дополнительного документа –

ИНН или СНИЛС). Ранее с помощью неидентифицированных электронных кошельков было запрещено осуществлять лишь расчеты за рубежом и между физическими лицами. Также неидентифицированные клиенты смогут «предоставлять денежные средства оператору электронных денежных средств только с использованием банковского счета» [4].

К тому же критически ограничены максимально возможные суммы обналичивания: не более 5 000 рублей в день или не более 40 000 рублей в месяц). Переводить же деньги на банковский счет в пользу юридических лиц и индивидуального предпринимателя допустимо только в том случае, если остаток средств на счету будет выше 60 тыс. рублей, при этом сумма перевода – не более 200 тыс. рублей в месяц.

По мнению председателя совета Ассоциации участников рынка электронных денег и денежных переводов В. Достова, такая жесткая политика государства приведет лишь к тому, что пользователи, а вслед на ними и криминальные элементы, начнут переходить на использование криптовалют или наличных денег. Это говорит о направленности данных жестких мер в первую очередь против добросовестных клиентов, и, следовательно, их неэффективности.

Аналогичного мнения придерживается и сервис «Яндекс.Деньги»: «Маленькие лимиты – в частности, на снятие наличных в пределах 5 000 рублей – делали анонимный кошелек удобным инструментом для небольших бытовых платежей, но непривлекательным для противоправных действий. Новые ограничения функций анонимных кошельков усложнят использование электронных денег».

Также ряд реформ принят и в области уголовной политики. С целью снизить привлекательность данных преступлений Федеральный Закон № 111-ФЗ от 23 апреля 2018 г., ст. 158 («Кража») и ст. 159.6 («Мошенничество в сфере компьютерной информации») гл. 21 УК РФ (Преступления против собственности) были дополнены таким квалифицирующим признаком, как «с банковского счета, а также в отношении электронных денежных средств». Данный признак был расположен в ч. 3 указанных статей, что повысило ответственность за данные преступления (максимальное наказание – до 6 лет лишения свободы) и перевести их в категорию тяжких. Этим же законом был расширен состав ст. 159.3 УК РФ: с «Мошенничества с использованием платежных карт» до «Мошенничества с использованием электронных средств платежа».

Еще в 2017 г. Пленумом Верховного Суда Российской Федерации в постановлении № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» установлено, что электронные денежные средства, наряду с иными безналичными денежными средствами, являются самостоятельным предметом кражи. Также данным постановлением было определено время окончания данных преступлений - с момента изъятия электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Однако вопрос о месте совершения преступления остался открытым. Согласно сложившейся практике и приоритетной позиции пленума Верховного Суда, местом окончания преступления необходимо считать место нахождения организации, в которых хранились электронные средства пострадавшего. Следовательно, уголовные дела должны рассматриваться в том регионе или районе, откуда

деньги похитили. Однако отсутствие нормативного закрепления данной позиции зачастую приводит к значительному расширению географии осуществления предварительного расследования.

Также данным постановлением не дано актуальное толкование ст. 159.3 УК РФ. Понятие «электронное средство платежа» (закреплено в Федеральном законе № 161-ФЗ «О национальной платежной системе») включает в себя помимо платежных карт также «Клиент-банк», электронные кошельки (например, Яндекс.Деньги, *WebMoney*) и др. Поэтому, исходя из буквального толкования закона, при квалификации важно учитывать, что состав данного преступления образуют мошеннические действия с использованием любых электронных средств платежа, в то время как толкование дано только относительно мошенничества с использованием платежных карт.

В постановлении описаны иные особенности квалификации. ППВС № 48 дает разъяснения по поводу отграничения состава мошенничества с использованием электронных средств платежа от кражи.

Во-первых, деяние следует квалифицировать как кражу, если наличные денежные средства были сняты без участия уполномоченного работника кредитной организации (т. е. деньги были сняты с карты с помощью банкомата).

Во-вторых, кража будет и в том случае, если держатель платежной карты сам передал злоумышленнику конфиденциальную информацию, необходимую для получения доступа к хранящимся на ней денежным средствам, под воздействием обмана или злоупотребления доверием.

Однако разъяснения о разграничении мошенничества и кражи в отношении безналичных денежных средств, содержащихся в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 с учетом актуальных изменений уголовного закона, могут вызвать на практике значительные трудности. К примеру, составление распоряжения о перечислении денежных средств с карты потерпевшего на карту виновного через онлайн-банк, пароль от которого был получен путем обмана или злоупотребления доверием, подпадает и под признаки ст. 159.3 УК РФ в части использования электронных средств платежа, и под признаки ст. 159.6, поскольку предполагает ввод компьютерной информации, а с точки зрения Пленума Верховного Суда Российской Федерации, должно быть квалифицировано как кража.

Тем не менее, несмотря на принятые меры, согласно материалам Адвокатской газеты (статья написана на основе расширенной статистики, предоставленной Генеральной прокуратурой Российской Федерации), количество преступлений в данной сфере продолжает увеличиваться, их раскрываемость снижаться [5]. По мнению специалистов, это обусловлено в первую очередь сложностью для понимания лицами, осуществляющими предварительное расследование, данных составов, и, следовательно, сложностью с квалификацией данных преступлений, их разграничением между собой, недостаточностью и неактуальностью толкования норм.

Помимо трудностей с квалификацией при расследовании данных преступлений зачастую возникают проблемы с проведением следственных действий, а также со сроками предварительного расследования [6–8].

Кроме проведения обычных следственных действий, вроде допроса потерпевшего, необходимо также получить показания сотрудников интернет-провайдера, причем, как ранее уже было отмечено, место совершения таких преступлений не определено и при этом может иметь обширную географию. Сложности возникают из-за того, что проведение таких следственных действий требует от расследующих лиц наличия специальных знаний, опыта и ресурсов.

Также зачастую необходимо проведение компьютерной экспертизы, причем из-за нехватки специалистов в государственных экспертных учреждениях она занимает много времени, что зачастую приводит к затягиванию сроков предварительного расследования.

Такое положение дел приводит к тому, что пострадавшие вынуждены прибегать к помощи специальных кибердетективных агентств для исследования киберследов хищений и сбора доказательств, а только потом уже обращаться в правоохранительные органы, чтобы избежать медленного непродуктивного расследования или вовсе отказа от возбуждения уголовного дела за отсутствием состава. Однако и в данной ситуации могут возникнуть проблемы с приобщением полученных кибердетективными агентствами доказательств к материалам уголовного дела, в частности, с допустимостью данных доказательств.

Именно со специфичностью понятийного аппарата и необходимостью проведения большого объема процессуальных действий специалисты связывают тенденции снижения раскрываемости данной категории преступлений. Эти же трудности, по их мнению, отталкивают недобросовестных следователей и дознавателей возбуждать уголовные дела.

Следовательно, можно выделить следующие тенденции в снижении количества преступлений, совершаемых с помощью электронных средств платежа, и повышению качества расследования данных преступлений:

Во-первых, необходимо более качественно регламентировать данную сферу преступлений, дополнить Уголовный кодекс составами пропорционально количеству существующих преступлений, ввести обновления в Уголовно-процессуальный кодекс Российской Федерации, а также, обобщив существующую судебную практику, дать более актуальное толкование по особенностям квалификации и разграничению уже существующих составов.

Во-вторых, необходимо повысить уровень компетентности сотрудников правоохранительных органов, в том числе сотрудников, осуществляющих предварительное расследование, увеличить количество экспертов, а также улучшить ресурсную базу, которую данные органы смогут использовать при расследовании.

По мнению А. Писемского, исполнительного директора *CSI Group*, полиция нуждается в высококлассных специалистах и современных инструментах для анализа цифровых доказательств и проведения расследований. Причем это направление требует существенного финансирования и создания условий для привлечения квалифицированных кадров не только в столицах, но и других регионах. Во многих странах мира следователи по *cybercrime* – это прежде всего технические эксперты с дополнительным юридическим образованием.

В-третьих, необходимо работать над предотвращением данного рода преступлений, в том числе и путем повышения киберграмотности населения, цифровой гигиены пользователей электронных систем платежа, осведомленности об угрозах, существующих в интернет-пространстве.

Только совокупность данных мер позволит реально сократить количество хищений и иной преступности, а также повысить качество расследования уже совершенных преступлений.

Список литературы

1. Меркулова И. В., Коркмазова А. Р. Электронные деньги в России: возникновение, развитие, проблемы и перспективы формирования // URL: http://www.rusnauka.com/20_DNI_2013/Economics/1_140878.doc.htm (дата обращения: 20.10.19).

2. Кондратьев П. В. Правовое регулирование оборота электронных денежных средств [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/problemy-informatsionno-pravovogo-regulirovaniya-elektronnyh-denezhnyh-sredstv (дата обращения: 20.10.19).

3. Официальный сайт Центрального банка Российской Федерации: Статистика: Основные показатели развития национальной платежной системы [Электронный ресурс] // URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet001.htm (дата обращения: 20.10.19).

4. Пункт 2 Федерального закона от 2 августа 2019 г. № 264-ФЗ «О внесении изменений в Федеральный закон “О национальной платежной системе”» [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_330671/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100021 (дата обращения: 20.10.19).

5. Адвокатская газета. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya (дата обращения: 20.10.19).

6. Мешков М. В. Досудебное соглашение о сотрудничестве: проблемы и перспективы / М. В. Мешков, В. В. Гончар // Закон и право. – 2011. – № 1. – С. 92-94.

7. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. –2019. – № 1. – С. 18–27.

8. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Кочеткова Елена Владимировна[1]*,*
курсант 374 взвода института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]*,*
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

АРМ СЛЕДОВАТЕЛЯ КАК СРЕДСТВО СОВЕРШЕНСТВОВАНИЯ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В настоящее время нам сложно представить работу сотрудников органов предварительного расследования без информационных технических средств, которые позволяют облегчить, значительно упростить и повысить эффективность и возможность наиболее быстрого расследования и раскрытия преступлений.

В данной статье хотелось бы осветить некоторые аспекты базы данных следователей (дознавателей), возможности данного программного продукта, их преимущество, удобство, эффективность работы, а также скорость выполнения поставленных задач перед следователем (дознавателем) при поиске информации о преступнике, привлечении лица к уголовной ответственности, планировании рабочего времени, создании запросов, протоколов, постановлений и иных процессуальных документов, необходимых при осуществлении процессуальных действий следователя (дознавателя).

Следует указать, что соответствующие базы данных не имеют особый успех в органах предварительного расследования, так как, в первую очередь, это обуславливается необходимостью ведения письменной документации, которая занимает большое количество времени, и дополнительная загруженность в виде электронных данных считается нецелесообразной по затрате времени для сотрудников.

Несмотря на это, мы считаем, что такие возможности интернет-ресурсов нельзя оставлять без внимания, и по возможности переходить на них, ведь это позволит значительно разгрузить объем работы и станет комплексным решением задач в деятельности следователя (дознавателя).

Далее мы представим наиболее популярную и освоенную базу данных следователей (дознавателей), способ работы с ней, как с помощью нее можно получить информацию о лице, привлеченным к уголовной ответственности, а также об уголовных делах, в которых фигурировало это лицо, и иную справочную информацию.

---

1. Программный комплекс «Автоматизированное рабочее место следователя (дознавателя)» – что это такое?

Программный комплекс «Автоматизированное рабочее место следователя (дознавателя)» – это современная, удобная информационно-техническая база данных для сотрудников органов юстиции и органов предварительного расследования для организации работы с информацией, имеющей важное значение по расследованию и раскрытию преступлений, которая оказывает большую помощь не только в следственной, но и в оперативно-разыскной деятельности.

Соответствующие базы данных начали разрабатывать в 1993–1996 гг. в Научно-исследовательском институте систем автоматизации (НИИСА), и они были предназначены для:

- Центрального аппарата Следственного комитета Российской Федерации;
- следственных управлений (отделов) МВД–УВД;
- следственных подразделений городских и районных органов внутренних дел.

В состав программного комплекса «АРМ следователя (дознавателя)» входит программа «Помощник следователя (дознавателя)», а также вспомогательное программное обеспечение, выполняющее отдельные задачи.

Основные возможности данной программы:

1. Полноценный, расширенный и быстрый доступ к различной справочной информации, правовой и методической литературе.
2. Ведение учетов материалов проверок, поручений и уголовных дел.
3. Планирование рабочего времени по группе дел.
4. Поиск материала уголовного дела.
5. Контроль сроков предварительного расследования.
6. Опись документов.
7. Работа с единой базой данных.
8. Автоматизация создания документов по информации из базы данных (запросы, протоколы, постановления, и т. д.).
9. Использование процессуальных шаблонов документов.

«АРМ следователя (дознавателя)» также позволяет ускорить и упростить процесс заполнения статистических карт установленных форм.

Хочу отметить, что один из авторов-разработчиков данного программного комплекса был следователем. Как показала практика, использование «АРМ следователя (дознавателя)» позволяет сэкономить до 50 % рабочего времени сотрудника. При необходимости создания большого количества процессуальных документов программа существенно помогает им в выполнении работы.

2. Система работы программы «Автоматизированное рабочее место следователя (дознавателя)

При регистрации пользователя в «АРМ следователя (дознавателя)» автоматически формируется папка с его фамилией с папкой «Уголовное дело № n».

В результате использования базы данных она непосредственно обеспечивает определенную защищенность материалов уголовных дел, документов предварительного следствия и иных процессуальных документов пользователей от несанкционированного и противоправного доступа.

Подводя итоги рассматриваемой темы моей статьи, я хочу сказать о действительной необходимости использования данных программных ресурсов, в нашем случае – «Автоматизированное рабочее место следователя (дознавателя)», в практической деятельности сотрудников правоохранительных органов и органов предварительного расследования. Мы наглядно можем убедиться в эффективности и целесообразности использования базы данных на регулярной основе, так как это позволяет улучшить, упростить, ускорить процесс работы с обширным объемом документации следователя (дознавателя). Путем внедрения информационных технологий в деятельность органов внутренних дел, мы сможем успешно повысить уровень раскрываемости преступлений, улучшить эффективность деятельности сотрудников МВД России, повысить качество и выполнение работы органов предварительного расследования. Несмотря на то, что в наше время при производстве уголовного дела используются в основном бумажные носители, такие программы, как «Автоматизированное рабочее место следователя (дознавателя)», имеют свое достоинство, простоту работы и способны сократить излишний документооборот в деятельности сотрудников.

Список литературы

1. Предварительное следствие в органах внутренних дел : учебное пособие / А. А. Орлова, В. В. Гончар, В. И. Батюк [и др.] ; под ред. М. В. Мешкова. – М. : Щит-М, 2007.

2. Программный комплекс «АРМ следователя (дознавателя)» [Электронный ресурс] // Разработка и дизайн сайта TS-Group. – URL: https://www.ts-group.ru/awp.php.

3. Гончар В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4 – С. 14–18.

4. Краткий обзор АРМ следователей [Электронный ресурс] // Инфопедия. – URL: https://infopedia.su/9xff73.html

5. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

6. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Куликова Маргарита Андреевна[1]**,**
курсант факультета подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Повышение эффективности работы правоохранительных органов по расследованию преступлений в настоящее время невозможно без интеграции новых информационных технологий. В современных условиях с развитием научно-технического прогресса информационные технологии являются неотъемлемой частью нашей повседневной жизни. Исходя из этого, продолжает быть актуальной деятельность по разработке современных эффективных средств и методов работы правоохранительных органов, способствующих расследованию преступлений.

Вместе с тем анализ складывающейся оперативной обстановки, связанной с IT-преступностью, свидетельствует о наличии ряда проблемных вопросов, препятствующих эффективной организации соответствующих направлений оперативно-служебной деятельности органов внутренних дел и требующих скорейшего разрешения.

Сохраняется возможность у лиц, занимающихся преступной деятельностью, избегать идентификации путем использования программных технологий *VPN*, *TOR*, *SSL*, позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров посредством SIP-телефонии.

Применяемые способы шифрования данных на распространенных интернет-сервисах не позволяют устанавливать IP-адреса серверов пользователей, отслеживать их активность, устанавливать данные пользователей. Существующий порядок оформления идентификационных модулей операторами сетей подвижной радиотелефонной связи порождает комплекс проблем, связанных с установлением абонента в процессе раскрытия преступлений.

До настоящего времени не завершен процесс формирования договорной правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисов, в том числе социальных сетей. Отдельного внимания заслуживает вопрос обеспечения доступа правоохранительных органов к идентификационным сведениям о лицах, совершивших платежные операции посредством банковских и иных платежных систем.

На сегодняшний день можно достаточно назвать направлений использования открытых информационных ресурсов в деятельности оперативных подразделений, подразделений предварительного расследования органов внутренних дел.

Руководствуясь в своей деятельности действующим законодательством Российской Федерации, правоохранительные органы с помощью официального интернет-портала правовой информации (*http://pravo.gov.ru*) могут оперативно получить доступ к постоянно меняющейся законодательной базе.

Благодаря сайту «Судебные и нормативные акты РФ» (*https://sudact.ru*) следователю доступна судебная практика по уголовным делам всех регионов России. Используя поисковую оболочку, на данном интернет-ресурсе можно найти приговоры и другие судебные решения по всем категориям уголовных дел, что дает возможность следователям в сложных ситуациях принятия процессуальных решений использовать опыт работы по расследованию аналогичных уголовных дел.

Общедоступная информация в цифровом виде востребована обществом для решения различных задач. Так, на сайте *https://гибдд.рф/check/auto* можно запросить информацию об истории регистрации транспортного средства в ГИБДД, участии в дорожно-транспортном происшествии, нахождения в розыске, наличии ограничений.

В настоящее время эффективным средством расследования преступлений является видеозапись. Так, на примере города Москвы можно просмотреть на сайте *http://youwebcams.net/online/category/russia/moscow* доступные в реальном времени веб-камеры, напрямую передающие все происходящее в Сеть.

Анализ информации, размещенной в сети Интернет, в том числе социальные сети, может помочь раскрытию и расследованию многих преступлений, обнаружению иных, неизвестных следствию источников информации и доказательств.

Информация, содержащаяся в аккаунтах социальных сетей, является важным объективным источником информации о личности как подозреваемых, так и иных участников судопроизводства. Фиксация факта общения в сети, наличия лиц в «друзьях», общие фотографии могут быть использованы для доказывания мотива преступления, наличия личной заинтересованности в ходе расследования и других обстоятельств или положены в основу принятия решения о производстве следственных действий (обыска, допроса, контроля и записи телефонных и иных переговоров и др.).

Не так давно компания «Яндекс» запустила сервис для поиска людей в социальных сетях по адресу *yandex.ru/people*. На сегодняшний день поиск можно осуществить по 16 соцсетям: «ВКонтакте», «Одноклассники», *Facebook*, *Beon* и др. Необходимо отметить, что поиск можно осуществлять не только по имени и фамилии, но и по никнейму или псевдониму.

Узнать, какие записи человек размещал за последнее время на *Facebook*, *Instagram* и других социальных сетях, можно с помощью программы *Social Searcher*.

Также, например, чтобы узнать, что постил человек в *Twitter* в конкретный день, в социальной сети есть специальный оператор для расширенного поиска

(например, *from:@tim_cook until:2019-10-17*), а с помощью оператора *near:* можно узнать, что пишут люди в конкретном городе или в точке с определенной широтой и долготой (например, *near:56.35,47.03*).

Чтобы получить информацию о человеке, можно воспользоваться сайтом *Social Mention*. На данном сайте мы узнаем, что пишут о человеке в социальных сетях.

Интернет-ресурсы позволяют получить нам необходимые и имеющие значение сведения о человеке по фотографиям. Так, обладая фотографией человека, возможно найти, где в сети Интернет размещена данная (или очень похожая) фотография. Для этого нужно добавить фотографию лица человека в поиск картинок в *Google*. На сайте *https://findclone.ru* при использовании фотографии можно осуществить поиск любого человека в социальной сети «ВКонтакте», а с помощью *Yomapic* можно увидеть, какие снимки были сделаны в определенном месте.

Имея информацию о человеке, а именно: имя, фамилия и регион прописки, можно посмотреть наличие у человека долгов перед государством с помощью базы СФПП.

Определение страны и региона по мобильному номеру телефона абонента сотовой и стационарной связи возможно на сайте *gsm-inform.ru*.

Определить физический адрес (местонахождение) человека по IP-адресу можно с помощью использования сайта *https://2ip.ru/geoip*. Для этого достаточно в поле ввести IP-адрес – данный ресурс выдаст информацию о местонахождении человека с точностью до координат.

Узнать адрес человека по номеру телефона или ФИО представляется возможным с помощью сайта *http://nomerorg.company* , где, выбрав интересующий город, в котором нужно найти человека, необходимо ввести фамилию, имя и отчество либо домашний номер телефона. После чего нужно открыть *Google Maps* и выяснить со спутника или по карте, где проживает интересующий человек. Обратным путем можно узнать домашний номер по адресу.

Таким образом, можно сказать, что целесообразность использования в расследовании преступлений сведений, размещенных на ресурсах сети Интернет обуславливается тем, что такого рода информация может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-разыскных и следственных мероприятий; поиск информации на открытых информационных ресурсах быстрее, а иногда и более эффективнее, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются средством быстрого получения необходимой информации. Социальные сети как инструмент в расследовании удобны своей доступностью, скоростью извлечения и объемом информации, которая может быть получена.

В настоящее время представляется целесообразным и важным разработать методические рекомендации для сотрудников правоохранительных органов, устанавливающих механизм поиска информации в сети Интернет.

Список литературы

1. Предварительное следствие в органах внутренних дел : учебное пособие / А. А. Орлова, В. В. Гончар, В. И. Батюк [и др.] ; под ред. М. В. Мешкова. – М. : Щит-М, 2007.

2. Смирнов И. В. Не надо разбрасываться своими персональными данными [Электронный ресурс] // URL: http://www.it-weekly.ru/it-news/security/135841.html.

3. Гончар В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4 – С. 14–18.

4. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

5. Котляров И. И., Пузырева Ю. В. Международное право и его роль в деятельности органов внутренних дел России / И. И. Котляров, Ю. В. Пузырева // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Марков Егор Ильич[1]**,**
заместитель командира взвода Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА И СУДЕБНО-СЛЕДСТВЕННАЯ ПРАКТИКА ПО СТ. 272 УК РФ

Из информации ГИЦ МВД России следует, что с каждым годом количество информационных преступлений только неумолимо растет, а преступность в информационной сфере процветает и имеет высокую степень латентности, поэтому с каждым годом уменьшается количество возбуждаемых уголовных дел по данным составам преступления. Поэтому правоохранительным органом и частным компаниям все тяжелее бороться с киберпреступниками, которых с каждым годом становится в разы больше, а способы совершения преступлений все сложнее. Вследствие этого для эффективной борьбы с преступлениями в информационной сфере и использованием технических средств государственным органам необходима современная техническая база, должное финансовое и материальное обеспечение, квалифицированные и подготовленные кадры. А также одно из самых главных – развитую и современную систему законодательства, которая не только идет в ногу со временем, но и опережает его. Поэтому законодательство, а именно гл. 28 УК РФ требует определенных доработок и повышения эффективности использования механизма уголовно-правового регулирования. Также факторами увеличения числа преступлений в сфере компьютерной информации являются неосведомленность и неграмотность определенной части населения нашей страны относительно процессов и сущности информационных компьютерных технологий, что приводит к неосторожности и небрежности при пользовании различными благами информационной среды, что впоследствии именно большинство видов компьютерный преступлений имеют возможность совершаться и существовать лишь благодаря данному фактору.

Ответственность за компьютерные преступления устанавливается Особенной частью разделом IX «Преступления против общественного порядка» гл. 28 («Преступления в сфере компьютерной информации») УК РФ, в которой содержится 4 состава: ст.ст. 272, 273, 274, 274.1. Рассмотрим ст. 272 УК РФ, так как в соответствии со статистическими данными за первое полугодие 2019 г. судебного департамента при Верховном Суде Российской Федерации подавляющее число осужденных приходится именно на данный состав преступления [1].

---

[1] © Марков Е. И., 2019.
[2] © Гончар В. В., 2019.

В ст. 272 УК РФ («Неправомерный доступ к компьютерной информации») объектом преступления являются охраняемые уголовным законом общественные отношения в сфере безопасной деятельности пользователей, владельцев и собственников информационных систем и ресурсов по созданию, сбору, обработке, накоплению, хранению, поиску, распространению и потреблению компьютерной информации. Факультативным признаком объекта в данном случае выступает предмет преступления. В настоящей статье им является компьютерная информация, которая представляет собой одну из разновидностей информации и нормативно закрепляется в Федеральном законе 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации» [2].

Согласно данному Федеральному закону, информация есть сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В соответствии с ч. 1 ст. 272 УК РФ информация – это информация на машинных носителях, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Системы ЭВМ – это комплексы, в которых хотя бы одна ЭВМ является элементом системы либо несколько ЭВМ составляют систему, а сети ЭВМ есть компьютеры, объединенные между собой линиями электросвязи. Под машинным носителем понимаются предметы, изготовленные из материала с определенными физическими свойствами, которые могут быть использованы для хранения информации и обеспечивают совместимость с устройствами записи – считывание данных. Объективная сторона преступления характеризуется общественно опасным деянием в форме действия, выраженного в неправомерном доступе к охраняемой законом компьютерной информации. Неправомерным доступом к компьютерной информации является несанкционированное со стороны владельца информации ознакомление преступника с данными, которые содержатся на машинных носителях или на ЭВМ. Общественно опасные последствия, которые выражаются в уничтожении, блокировании, модификации либо копировании информации, нарушении работы ЭВМ, системы ЭВМ или их сети.

Уничтожение информации – это совокупность последовательных операций, которые предназначены для осуществления программными или иными средствами необратимого удаления данных, в том числе и остаточной информации.

Блокирование информации – это запрет на выполнение последующих операций до завершения выполнения текущей либо запрет дальнейшего выполнения последовательности команд, или выключение из работы какого-либо устройства ЭВМ, а также это результат воздействия на ЭВМ и ее элементы, повлекшего временную или постоянную невозможность осуществления каких-либо операций над компьютерной информацией [3]. Достоинством данного определения является то, что блокирование информации рассматривается в виде результата непосредственного преступного воздействия на компьютерную информацию.

Копирование информации – это незаконное изготовление повторного и устойчивого экземпляра базы данных или файлов в любой материальной форме с последующих записях в запоминающее устройство ЭВМ.

Нарушение работы ЭВМ, системы ЭВМ либо их сетей может быть выражено посредством произвольного их отключения, независимого от собственника или

в отказе либо в неправильной выдаче определенной информации, при этом сохраняется целостность ЭВМ и их сетей, во временном или устойчивом создании помех для их функционирования в соответствии с назначением [4].

Причинно-следственная связь выражена в объективно существующей связи между общественно опасным деянием и наступившими общественно опасными последствиями.

Субъектом преступления является вменяемое физическое лицо, достигшее возраста уголовной ответственности, в данном случае шестнадцатилетнего возраста.

Субъективная сторона преступления характеризуется исключительно умышленной формой вины, которая может быть выражена как в прямом, так и в косвенном умысле. Субъект преступления осознает общественную опасность осуществляемого им неправомерного доступа к охраняемой законом компьютерной информации, предвидит возможность или неизбежность наступления в результате этого любого из перечисленных в диспозиции альтернативных последствий, указанных в ч. 1 ст. 272 УК РФ и желает их наступления либо не желает, но сознательно допускает эти последствия или безразлично относится к их наступлению. По конструкции данный состав преступления является материальным, таким образом, преступление считается оконченным с момента наступления альтернативных последствий, указанных в диспозиции настоящей статьи.

На сегодняшний день подавляющее большинство банков и кредитных организаций имеют программы банковского банкинга, с помощью которых пользователь с мобильного устройства (смартфон, планшет, смарт-часы и т. д.) может производить различные операции по своему счету в реальном времени, при подключении сети Интернет или же посредством СМС-сообщений. При этом некоторые операторы сотовой связи после смены номера или при отказе владельца от его использования, не отвязывают привязку номера телефона от банковского счета. После этого сотовый оператор может продать данный номер следующему клиенту, который таким образом получает возможность выполнять некоторые удаленные операции по счету, в том числе осуществлять банковские транзакции, без участия реального владельца счета. В таких случаях может иметь место внезапно возникший умысел, так как лицо может неумышленно приобрести у компании, оказывающую услуги связи, SIM-карту с номером, привязанным к банковскому счету прежнего владельца, но после прихода СМС-уведомления от банка, например, о совершении какой-либо банковской операции, которые зачастую рассылаются пользователям, осознает, что номер используется в качестве привязки к какому-либо пользователю банка, как раз после этого у данного лица может возникнуть умысел на совершение преступления. В этом случае злоумышленники снимают денежные средства небольшими суммами для того, чтобы банк не заблокировал данные операции как подозрительные. В настоящее время все банки имеют систему *3D-Secure*, которая представляет собой защищенный протокол для пользователей *CNP* – операций без присутствия карты (чаще всего используется для оплаты в интернет-магазинах, при этом покупатель для оплаты вводит реквизиты банковской карты), который добавляет дополнительный шаг для проведения оплаты, который заключается в отправке банковской организацией специально-

го кода-подтверждения (может отправляться по СМС-сообщениям либо уведомлением в мобильное приложение банка, который необходимо ввести для проведения транзакции. Очень важно, чтобы интернет-сайт и банк были обоюдно подключены к протоколу *3D-Secure* [5].

Итак, вернемся к передаче номера телефона другому пользователю сотового оператора. При использовании протокола *3D-Secure* это код безопасности от банковской организации приходит преступнику, а не старому владельцу номера, который вводит его при оплате товаров и услуг, имея лишь данные вашей карты, которые в том числе могут сохраняться на различных сайтах и доступом к номеру мобильного телефона. Такие вышеописанные преступные действия мошенников надлежит квалифицировать по ст. 272 и ст. 159 УК РФ. Также можно обратиться к судебной практике.

Из приговора № 1-287/12 от 19 октября 2012 г. по делу № 1-287/12 Свердловского районного суда г. Белгорода следует: Т., находясь в зоне действия базовой станции сотовой связи, действуя с единым преступным умыслом, направленным на хищение чужого имущества, из корыстных побуждений, используя абонентский номер гражданина И. (который не предоставлял законного права использовать информацию по его банковской карте третьим лицам), подключенный к банковской карте, осознавая, что имеет неправомерный доступ к охраняемой законом компьютерной информации – данным, находившимся на лицевом счете денежным средствам, сформировал и направил на специальный номер оператора мобильной связи БМБ-сообщение для перевода денежных средств на счет мобильного телефона, предоставленное в форме электрического сигнала, осуществив копирование информации с лицевого счета банковской карты И., с последующей модификацией, выраженной в изменении первоначальных данных по движению денежных средств по счету, незаконно списав с лицевого счета банковской карты в свою пользу денежные средства, принадлежащие И., осуществив неправомерный доступ к охраняемой законом компьютерной информации, т. е. произвел ее копирование и модификацию из корыстной заинтересованности. Данные действия суд квалифицировал по п. «в» ч. 2 ст. 158, ч. 2 ст. 272 УК РФ [6].

Стоит отметить, что ст. 272 не предъявляет требований к «вредоносности» модифицированной информации, т. е. действия преступника будут квалифицироваться по вышеупомянутой статье вне зависимости от причиненного им ущерба [7]. Также, соглашаясь с суждением Ю. И. Ляпунова, считаем, что моментом окончания доступа к компьютерной информации будет «момент отсылки пользователем компьютеру последней интерфейсной команды (голосовой, нажатием клавиши и т. п.) вызова хранящейся информации, независимо от наступления дальнейших последствий» [8]. Преступлением это деяние станет только при наступлении указанных в диспозиции последствий. Все действия, выполненные до подачи последней команды, будут образовывать состав неоконченного преступления [9–12].

Таким образом, можно с уверенностью говорить, что несогласованность действий кредитных организаций и компаний, предоставляющих услуги сотовой связи, а также невнимательность их клиентов ставят под угрозу безопасность банковский счетов людей, сменивших мобильного оператора, что

развязывает руки и дает возможность для роста преступности в данной сфере. Поэтому необходимо в первую очередь обязать операторов сотовой связи сообщать банковским организациям информацию о смене номера или отказе от номера клиента. При этом банк или сотовый оператор должны известить клиента о том, что его номер телефона привязан к его банковским данным и этим могут воспользоваться злоумышленники. Также считаем необходимым введение в средних образовательных организациях (школах, лицеях, гимназиях, колледжах) занятий по информационной безопасности, так как зачастую дети начинают пользоваться сетью Интернет, компьютером и другими устройствами довольно в раннем возрасте. Вторым фактором является то, что возможность получить дебетовую банковскую карту у граждан Российской Федерации появляется по достижении восемнадцатилетнего возраста. Другая необходимая мера: издание постановления пленума Верховного Суда Российской Федерации касаемо преступлений в сфере компьютерной информации, необходимость которого созревает в течение многих лет и всеми без исключения признается целесообразным.

Библиографический список

1. Судебный департамент при Верховном Суде Российской Федерации [Электронный ресурс] // URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 21.10.2019).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // URL: https://rg.ru/2006/07/29/informacia-dok.html (дата обращения: 20.10.2019).

3. Крылов В. В. Информационные компьютерные преступления : учебное и практическое пособие. – М. : Инфра-М ; Норма, 1997. – С. 52.

4. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» № 149-ФЗ (ред. от 18.03.2019) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru (дата обращения: 16.10.2019).

5. Банки.ру [Электронный ресурс] // URL: https://www.banki.ru/wikibank/3d-secure (дата обращения: 20.10.2019).

6. Судебные и нормативные акты Российской Федерации [Электронный ресурс] // URL: https://sudact.ru/regular/doc/Vegz2QhJyTY9 (дата обращения: 22.10.2019).

7. Дворецкий М. Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса Российской Федерации // Вестник Тамбовского университета. – Серия: Гуманитарные науки. – 2013. – № 12 (128). – С. 529.

8. Ляпунов Ю. И. Ответственность за компьютерные преступления // Законность. – 1997. – № 1. – С. 157.

9. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельности:

Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

10. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий /// Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

11. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

12. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / И. И. Котляров, Ю. В. Пузырева // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Мысина Анастасия Ильинична[1]**,**
адъюнкт второго года обучения
факультета подготовки научно-педагогических и научных кадров
Московского университета МВД России имени В.Я. Кикотя

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ПРОТИВОДЕЙСТВИЮ КОМПРОМЕТАЦИИ ДЕЛОВОЙ ЭЛЕКТРОННОЙ ПОЧТЫ

В настоящее время компрометация деловой электронной почты является одним из наиболее экономичных и распространенных видов преступлений в сфере информационных технологий. Следует отметить, что в контексте борьбы с киберпреступностью противоправные деяния подобного рода представляют собой далеко не новое явление. Однако общественная опасность и ущерб, причиненный в результате совершения актов компрометации деловой электронной почты, ежегодно стремительно возрастает, что в свою очередь требует совершенствования механизмов противодействия обозначенным преступлениям. Отдельного внимания заслуживает необходимость международного сотрудничества в борьбе с компрометацией деловой электронной почты, поскольку увеличивается количество случаев, когда рассматриваемые противоправные деяния: совершаются более чем в одном государстве; совершаются в одном государстве, но существенная часть подготовки, планирования, руководства или контроля имеет место в другом государстве; совершаются в одном государстве, но при участии организованной преступной группы, которая осуществляет преступную деятельность в более чем одном государстве; совершаются в одном государстве, но его существенные последствия имеют место в другом государстве. Это свидетельствует о транснациональном характере указанных противоправных деяний.

Компрометация деловой электронной почты представляет собой атаку, при помощи которой злоумышленник получает доступ к учетной записи электронной почты, чтобы в дальнейшем использовать ее в преступных целях (чаще всего для совершения мошенничества с применением методов социальной инженерии [1, 2]). Так, киберпреступник может рассылать вредоносное программное обеспечение, спам или фишинговые сообщения от имени директора, бухгалтера той или иной компании, представителей различных органов государственной власти и международных организаций и т. д. В качестве одного из вариантов подобных атак может выступать использование специального аккаунта с почтовым адресом, похожим на оригинальный адрес руководителя или одного из коллег [3]. В целом, компрометация деловой электронной почты является одним из видов мошенничества с использованием информационных технологий и является уголовно наказуемой в большинстве современных государств.

Стандартная схема совершения атаки компрометации деловой электронной почты включает три основных этапа:

1. Незаконный доступ (преступники совершают кибератаки в целях получения данных учетной записи жертвы).

2. Использование методов социальной инженерии (например, преступники от имени других сотрудников убеждают жертву совершить ту или иную транзакцию).

3. В ответ на полученную просьбу жертва совершает запрашиваемое действие (например, оплату тех или иных услуг).

В целях профилактики различных актов совершения компрометации деловой электронной почты необходимо:

1) использовать антивирус, брандмауэр;

2) регулярно обновлять программное обеспечение служебных, персональных компьютеров и иных используемых устройств;

3) обращать внимание на предупреждения системы безопасности, исправлять возникающие ошибки;

4) использовать спам-фильтры, блокировать доступ к подозрительным сайтам.

В контексте международного сотрудничества по противодействию компрометации деловой электронной почты большое значение имеет международно-правовое регулирование рассматриваемой сферы.

Так, представляется сообразным обратить внимание на то, что компрометация деловой электронной почты прямо не упоминается, но тем не менее находит отражение в различных международных договорах, посвященных вопросам транснационального сотрудничества по противодействию преступлениям в сфере информационных технологий.

В частности, в ст. 8 Конвенции Совета Европы о киберпреступности 2001 г. закреплено обязательство государств – участников квалифицировать в качестве преступления различные акты мошенничества с использованием компьютерных технологий [4].

Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2012 г. в ст. 11 также предусматривает криминализацию мошенничества [5].

В ст. 30 Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 г. установлено обязательство относительно криминализации мошенничества с использованием компьютерных данных [6].

Таким образом, необходимо отметить, что компрометация деловой электронной почты находит свое отражение в различных международно-правовых актах, поскольку выступает одним из видов мошенничества с использованием информационных технологий. Тем не менее в тексте положений обозначенных источников международного права отсутствуют непосредственные упоминания о компрометации деловой электронной почты, отсутствуют положения, детализирующие указанную сферу международно-правового регулирования.

Что касается сотрудничества государств по противодействию компрометации деловой электронной почты в рамках международных правоохранительных организаций, необходимо отметить следующее.

Так, международная организация уголовной полиции Интерпол проводит компанию *BECareful* в целях информирования мирового сообщества об увеличении количества актов компрометации деловой электронной почты, а также о мерах противодействия обозначенной угрозе. По данным Интерпола за

2018 г., ущерб, причиненный в результате совершения подобного рода преступлений, составил более 1 млрд долларов.

Информационная кампания *BECareful* сосредоточена на трех ключевых областях:

1) общая информация относительно компрометации деловой электронной почты;

2) советы о том, как определить потенциально мошеннический запрос и не стать жертвой компрометации деловой электронной почты;

3) советы по кибербезопасности для защиты компьютерных систем от вторжений [7].

Что касается международных операций, проводимых под эгидой Интерпола в рамках противодействия компрометации деловой электронной почты, следует обратить внимание на операцию «Ворон». Она инициирована в 2018 г. после того, как компания в Норвегии стала жертвой подобного рода преступлений и потеряла более 110 000 евро. В ходе расследований, проведенных в Норвегии, были установлены связи между этим делом и несколькими другими схожими по всей Европе. В октябре 2018 г. подразделение Интерпола по финансовым преступлениям организовало координационное совещание. Кроме того, подразделение Интерпола по киберпреступности провело анализ данных, собранных следователями, и подготовило отчеты о киберпреступности в целях оказания содействия расследованиям. В результате проведенной операции в Нигерии был задержан ряд подозреваемых, а также их сообщников. Представители власти Нигерии полагают, что злоумышленники имели доступ к нескольким банковским счетам для получения и отмывания доходов, около 3 млн долларов США в дальнейшем предположительно были направлены на финансирование преступной деятельности [8].

Рассматривая вопросы международного сотрудничества государств по противодействию компрометации деловой электронной почты в рамках Европола, необходимо отметить, что по данным Европейского центра киберпреступности с декабря 2016 г. по май 2018 г. рост преступности, связанной с компрометацией деловой электронной почтой, составил 136 %. Подобные атаки варьируются в зависимости от используемых инструментов. Одни успешно осуществляются при помощи методов социальной инженерии, в то время как другие применяют, например, вредоносное программное обеспечение. В связи с этим в современных условиях развития общества требуется выработка эффективных комплексных мер противодействия компрометации деловой электронной почты [9, 10].

Подводя итоги изложенного выше, представляется сообразным сделать вывод о том, что в современных условиях развития общества компрометация деловой электронной почты стремительно набирает обороты и все чаще приобретает транснациональный характер. Международные договоры, посвященные вопросам противодействия преступлениям в сфере информационных технологий, не детализируют особенности транснационального сотрудничества по вопросам, касающимся заявленной проблематики. Тем не менее государства в рамках международных правоохранительных организации активно сотрудничают по вопросам противодействия компрометации деловой электронной по-

чты. В связи с этим мы предлагаем закрепить на международно-правовом уровне понятие «компрометация деловой электронной почты» с целью обеспечения единообразия подходов к пониманию особенностей реализации межгосударственного взаимодействия в борьбе с рассматриваемыми преступлениями.

Список литературы

1. Гончар В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4 – С. 14–18.

2. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

3. BEC-атака [Электронный ресурс] // Глоссарий: Энциклопедия «Касперского» // URL: https://encyclopedia.kaspersky.ru/glossary/bec (дата обращения: 21.10.2019).

4. Конвенция Совета Европы о киберпреступности 2001 г. [Электронный ресурс] // Справочно-правовая система «ГАРАНТ». – URL: http://base.garant.ru/4089723 (дата обращения: 21.10.2019).

5. Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2012 г. [Электронный ресурс] // URL: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (дата обращения: 21.10.2019).

6. Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. [Электронный ресурс] // URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 21.10.2019).

7. INTERPOL urges public to #BECareful of BEC fraud [Электронный ресурс] // News: News-and-Events: Официальный сайт Интерпола. – URL: https://www.interpol.int/News-and-Events/News/2019/INTERPOL-urges-public-to-BECareful-of-BEC-fraud (дата обращения: 23.10.2019).

8. Global information exchange helps Nigeria nab online scammer [Электронный ресурс] // 2019: News: News-and-Events: Официальный сайт Интерпола. – URL: https://www.interpol.int/News-and-Events/News/2019/Global-information-exchange-helps-Nigeria-nab-online-scammerBECareful-of-BEC-fraud (дата обращения: 23.10.2019).

9. INTERNET ORGANISED CRIME THREAT ASSESSMENT 2019 [Электронный ресурс] // main-reports: activities-services: Официальный сайт Европола. – URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment ; file:///F:/Downloads/iocta_2019%20(1).pdf (дата обращения: 23.10.2019).

10. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Николаева Ангелина Владимировна[1]***,***
курсант 372 взвода института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]***,***
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПНОСТИ

Наше общество динамично, оно не стоит на месте, а находится в постоянном развитии, о чем свидетельствует множество открытий в различных сферах жизни. Не стоит на месте и мир преступности. С развитием компьютерных технологий, происходит модернизация криминальной деятельности. Сегодня все чаще и чаще наблюдаются преступления с использованием различного вида технических новшеств, что подтверждается возникновением ряда новых составов преступлений в УК РФ. Все эти новшества заставляют искать и использовать иные, обновленные способы расследования.

Всем нам известно, что в XXI в. информация представляет огромнейшую ценность для каждого из нас. Не зря существует суждение: «Человек, владеющий информацией, владеет миром». Именно поэтому преступления, связанные с посягательством на информацию, стали не редкостью в третьем тысячелетии, а угроза информационной безопасности стала одной из самых актуальных проблем на сегодняшний день, ведь большинство различной конфиденциальной информации граждан хранится в электронном виде в сети Интернет. Понятие «угрозы информационной безопасности» определяется в п. 2 «б» гл. I Доктрины информационной безопасности: «Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [1].

Европейская Конвенция Совета Европы по киберпреступлениям (преступлениям в киберпространстве) от 23 ноября 2001 г. подразделяет киберпреступления на четыре типа:

1. «Незаконный доступ – ст.2 (Умышленный противоправный доступ к компьютерной системе либо ее части).

2. Незаконный перехват – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах).

3. Вмешательство в данные – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных).

4. Вмешательство в систему – ст. 5 (противоправное препятствование функционированию компьютерной системы путем ввода, передачи, поврежде-

ния, удаления, нарушения, изменения либо пресечения компьютерных данных)».

С расширением применений новых технологий в информационной сфере, являющимися непосредственным фактором развития экономики, а также совершенствования функционирования институтов общества и государства одновременно возникают новые информационные угрозы, для предотвращения которых необходимы новейшие методы борьбы, поскольку большинство преступлений, которые совершены в глобальных компьютерных сетях, обладают рядом специфических особенностей, таких как:

1. Высокая скрытность, которая обеспечивается своеобразием сетевого информационного пространства.
2. Совершение преступлений хорошо подготовленными преступниками, обладающими высоким интеллектом, который усложняет характер преступной деятельности.
3. Использование абсолютно новых, сложных и обновленных способов совершения преступления.
4. Осуществление преступной деятельности дистанционно.
5. Предотвращение возможности использования обыденных методов борьбы с данным видом преступлений.
6. Применение автоматизированного режима в совершении преступления, позволяющего совершать преступление сразу в нескольких местах и многое другое.

Именно поэтому важно обеспечивать эффективное и грамотное противодействие данным видам преступлений. Чтобы сделать это, необходимо осуществление ряда следственных действий, формирующих доказательственную базу в ходе ведения уголовных дел такого характера.

Итак, киберпреступность – это один из видов правонарушений, осуществляемый путем применения компьютерных технологий, включающий в себя распространение вирусов, нелегальную загрузку файлов, а также персональной информации: информации по банковским счетам.

Данный вид преступности растет не только в пределах нашего государства, интернет-преступность охватывает и международные масштабы, о чем свидетельствуют данные многих известных международных компаний, а также выводы экспертов и аналитиков. По данным компании *Allianz Global Corporate & Specialty,* в 2016 г. ущерб от данного вида преступности для мировой экономики превысил 575 млрд долларов, что составляет около 1 % мирового ВВП. В 2018 г. ущерб мировой экономике от участившихся кибератак, по прогнозам Сбербанка России, вырос практически в два раза по сравнению с предыдущим годом. По расчетам *Allianz Global Corporate & Specialty*, действия хакеров приносят наибольший вред мировой экономике [2]. Например, недавно хакеры осуществили взлом и раскрыли личные данные более 200 млн человек американского бюро кредитных историй *Equifax* и *Uber*, принеся этим компаниям огромный убыток. На сегодняшний день киберпреступность значительно выросла в сравнении с предыдущим годом: так, за первые восемь месяцев 2019 г.

Генеральной прокуратурой Российской Федерации зарегистрировано около 180 153 киберпреступлений, что на 66,8 % больше предыдущего года [3].

Для снижения роста данного вида преступности борьбу с ней необходимо осуществлять как на внешнегосударственном уровне, так и непосредственно внутри стран. Именно поэтому очень важно иметь компетентных сотрудников МВД России, наделенных специальными знаниями и навыками, для расследования такого рода преступлений на территории нашего государства. Безусловно, работа с доказательствами на электронных носителях информации должна осуществляться специалистами, но не всегда это возможно, поскольку очень часто имеет место недобор сотрудников в отделениях полиции, тогда вся работа ложится на плечи следователя.

Зачастую обыденного опыта следователя может не хватать при расследовании преступлений в сфере информационных технологий. Именно поэтому в настоящее время, время информационных открытий, очень важен высокий уровень подготовленности и профессионализма следователей, которые в ходе получения доказательств по уголовному делу, обязаны самостоятельно грамотно осуществлять ряд следственных действий, направленных на извлечение нужной информации с различного рода компьютерной техники.

Существует большое количество различного рода следственных действий, в том числе и в применении к расследованию киберпреступлений. Так, к ним можно отнести: назначение компьютерно-технической экспертизы, обыск, следственный эксперимент и др. Особое значение для выявления следов преступления с использованием ЭВМ имеют осмотр и выемка электронных носителей информации, ведь особенностью киберпреступлений является то, что большинство следов преступлений нельзя выявить и воспринять без использования специального программного обеспечения и специальных аппаратов.

В ходе осуществления такого следственного действия, как осмотр места происшествия, которое является основополагающим и начальным этапом расследования, своевременное выявление, фиксация, изъятие, изучение, а также предварительное исследование в установленном законом порядке необходимой информации – являются непосредственной задачей осмотра места происшествия при расследовании преступлений в сфере информационных технологий. Осмотр, его основания и порядок регламентируется ст.ст. 176–177 УПК РФ [4].

Порядок данного следственного действия при расследовании киберпреступлений должен начинаться прежде всего с того, что, прибыв на место происшествия, следователь должен выполнить ряд важных действий, направленных на обеспечение сохранности следов преступления, а также обстановки, при которой оно было совершено. Для этого необходимо оцепить территорию, на которой произошло общественно опасное деяние, а также исключить проход посторонних лиц на нее, поскольку очень важно сохранить первоначальный облик объектов места преступления. Например, если ПК был включен, его необходимо оставить в таком же состоянии и наоборот, если он выключен. Далее следователю необходимо в ходе проведения опроса детально зафиксировать в протоколе все сведения, которые будут получены от потерпевших (потерпевшего, заявителя), а также подробно зафиксировать обстановку места происшествия, осмотрев его.

В ходе осуществления данного следственного действия очень важно использовать тактику «от центра – к периферии», о чем говорит специалист в области компьютерных технологий Д. А. Илюшин. Так, если преступление было совершено посредством ПК, первоначально важно провести обзорный осмотр, т. е. осмотреть помещение, в котором распложен ПК, выявить наличие локальных сетей, а затем детальный осмотр рабочего места, его внешний облик на выявление на клавиатуре или на других местах отпечатков пальцев, волос, частичек кожи и других следов. Следующими необходимо исследовать ПК. Начиная с его включения, необходимо определить вид операционной системы компьютера, какие программы использовались в ходе выполнения последних операций на нем, а также информацию, находящуюся компьютере, которая явилась предметом преступления, а также осмотреть место хранения и обработки информации для выявления виртуальных следов.

Ни для кого не секрет, что большинство кибепреступлений, направленных на получение и использование конфиденциальной информации, осуществляются в удаленном доступе, что усложняет ход расследования. В таком случае с целью удержания и сохранения данных последнего сеанса важно осуществить блокировку работающих программ, что достаточно сложно без квалифицированного специалиста в области компьютерных технологий. Специалисту необходимо произвести осмотр ПК на наличие вредоносных программ, средств защиты информации, а также удаленного доступа. Если все они имеются на ПК, важно своевременно отключить их, блокировать на компьютере удаленный доступ, поскольку преступник может произвести любые действия в удаленном доступе, очистив важную, имеющую значение для следствия информацию. В качестве примера рассмотрим программу *LiteManager Pro,* с помощью которой преступник может осуществлять управление компьютером: его питанием – отключать или включать, перезагружать ПК, производить блокировку клавиатуры, монитора, находясь в любом месте, с использованием функцией *Wake-On-LAN*. Преступник также может просмотреть любую информацию, находящуюся на обыскиваемом компьютере и произвести многие другие операции.

По окончании проведения обзорного осмотра помещения важно изобразить некую схему, где будут определены места расположения оборудования, с помощью которого было совершено преступление, а также сети и точки связи с удаленными системами [5].

Немаловажным следственным действием, которое определено в ст. 183 УПК РФ, выступает выемка – следственное действие, основная цель которого – изъятие определенных предметов и документов, имеющих значение для уголовного дела. Выемка довольно похожа на следственное действие обыск, но есть некие отличия, которые состоят в том, то при производстве первого заранее известен характер изымаемых предметов, а также их место нахождения [6]. Изъятие предметов возможно двумя способами: путем добровольной выдачи или же принудительной (ч. 5 ст. 183 УПК РФ).

Выемка помогает произвести работу с электронным источником, в том числе и его осмотр в удаленном от места происшествия месте, поскольку очень часто сделать это на территории, где произошло преступление, попросту не имеется

возможным. Так, очень часто производят изъятие жестких дисков, флеш-карт, файлы из памяти ПК, информацию с сайтов и социальных сетей сети Интернет, а также сам компьютер и различного рода мобильные устройства. Основным и важным условием проведение выемки выступает участие в нем специалиста, что закреплено в ч. 1 ст. 58 УПК РФ: «… лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном УПК РФ, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела». Обусловлено это тем, что обеспечить грамотное изъятие с соблюдением прав и законных интересов владельцев электронной информации достаточно сложно, в той же мере, которую составляет техническая сложность осуществления этого следственного действия.

Говоря о производстве отдельных процессуальных действий, необходимо сказать о том, что большое значение в ходе их производства имеет такое направление в криминалистике как форензика, другими словами – компьютерная криминалистика – прикладная наука о раскрытии и расследовании преступлений в сфере компьютерной информации, связанная с исследованием следообразования, цифровых доказательств, а также методов их выявления и различного рода технических средств, используемых в ходе совершения и расследования преступления. Так, очень часто преступники производят установку поля из электромагнитных лучей в помещении или же на входе в него для повреждения информации, хранящейся на электронных носителях. Для этого важно правильно упаковать его, к примеру, если это жесткий диск, то его необходимо поместить в светоотражающий алюминиевый бокс или же в фольгу в три слоя [7]. К тому же форензика представляет большое количество технических средств, упрощающих работу специалиста, например, такие криминалистические инструменты как:

1) «устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях);

2) устройства для подключения исследуемых дисков с аппаратной блокировкой записи на них;

3) программные инструменты для криминалистического исследования содержимого дисков и других носителей, а также их образов;

4) переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях;

5) наборы хэшей (*hash sets*) для фильтрации содержимого изучаемой файловой системы;

6) аппаратные и программные средства для исследования мобильных телефонов и сим-карт [W01, 60, 90];

7) программные средства для исследования локальных сетей и многие другие» [5].

Таким образом, осмотр и выемка – это процессуальные действия, грамотное проведение которых становится неотъемлемым условием сбора, а также должного хранения доказательств, имеющих важное значение для расследования. Но

очень часто на практике имеются некие сложности, заключающиеся в отсутствии у следователя определенных навыков работы с информационными технологиями, что достаточно усложняет проведение ряда процессуальных действий и становится неким барьером в ходе разрешении дела [8]. Именно поэтому с целью наиболее оперативного производства следственных мероприятий необходимо искать пути разрешения данной проблемы в будущем, обеспечив прохождение обучения работе с электронными источниками информации следователям, а также грамотного осуществления процессуальных действий в ходе расследования киберпреступлений с минимальным обращением за помощью к специалистам.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 02.08.2019).

2. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. – №646. – п. 2, б) гл. I.

3. Портал правовой статистики Генеральной прокуратуры Российской Федерации [Электронный ресурс] // URL: http://crimestat.ru/offenses_chart.

4. Allianz Global Corporate & Specialty: О развивающихся угрозах и рисках, связанных с кибератаками [Электронный ресурс] // URL: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html.

5. Федотов Н. Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

6. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–132.

7. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

8. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Орлова Алла Алексеевна[1]***,***
главный научный сотрудник
НИЦ № 5 ФГКУ «ВНИИ МВД России»,
доктор юридических наук, доцент

ОТДЕЛЬНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ ИЗ БАНКОВСКИХ АВТОМАТИЧЕСКИХ ТЕРМИНАЛОВ САМООБСЛУЖИВАНИЯ

С развитием банковской системы и электронных технологий, в период повсеместного распространения безналичных расчетов и электронных платежных систем, банкоматы, как один из основных элементов автоматизации процессов банковских операций, все чаще используются для совершения преступлений.

Следует подчеркнуть, что ввиду многообразия проявлений признаков объективной и субъективной стороны совершаемых в указанной сфере преступлений, правоприменительная практика сталкивается с целым рядом сложностей, связанных не только с квалификацией противоправных действий, но и со своевременным и правильным выявлением способа получения неправомерного доступа к сведениям, составляющим налоговую [1], коммерческую [2] или банковскую [3] тайну юридических и физических лиц с целью последующих хищений их денежных средств, с надлежащим процессуальным оформлением полученной информации, с доказыванием обстоятельств, предусмотренных в ст. 73 УПК РФ.

Остановимся лишь на некоторых из обозначенных аспектов проблемы.

Одним из способов получения персональных данных и хищений денежных средств граждан является установка на банкоматы так называемого *внештатного оборудования*. При этом наиболее распространенным способом получения персональных данных клиентов небезосновательно считается *скимминг.*

Под *скиммингом* следует понимать копирование данных путем установки перед картридером[2] специального устройства – «*скиммера*». Данное устройство по своему внешнему виду имитирует стандартное оборудование банкомата и визуально не распознается лицом, желающим получить принадлежащие ему денежные средства из банкомата по персонифицированной банковской карте.

Как правило, сбор сведений о персональных данных владельцев банковских карт, а также сведения об их ПИН-кодах осуществляются для последующего хищения денежных средств со счетов граждан – владельцев скомпрометированных карт.

Следовательно, при проверке заявлений и сообщений о преступлениях, связанных с хищением из банкоматов или с их использованием путем *скимминга* органам предварительного расследования необходимо учитывать целый ряд обстоятельств, позволяющих ориентироваться в вопросах установки и использо-

---

[1] © Орлова А. А., 2019.

[2] Под картридером понимается небольшое по размеру устройство, предназначенное для быстрого считывания карт памяти, *compact flash*-карточек и других типов памяти.

вания указанного вида внештатного оборудования, а также его обнаружения и надлежащей процессуальной фиксации полученных результатов.

Как правило, факты, свидетельствующие об установке *скиммера* на банкомате, выявляются сотрудниками банков при их осмотре, а также в результате обращений пострадавших граждан о хищении денежных средств.

Совокупность первоначальных процессуальных действий и организационных мероприятий при наличии надлежащего, предусмотренного в ст. 140 УПК РФ повода для возбуждения уголовного дела, включает в себя: выезд следственно-оперативной группы на место совершения преступления; получение объяснений; истребование и получение сведений о движении денежных средств по соответствующим банковским счетам; проведение осмотра места происшествия.

Принимая во внимание, что выезд на место происшествия предполагает выполнение действий, связанных с высокотехнологичным оборудованием, а обнаружение и изъятие значимых для расследования преступления предметов требует специальной подготовки и должной квалификации, результаты производимых мероприятий определяются не только квалификацией следователя, но и уровнем и профилем профессиональной подготовки соответствующего специалиста, что необходимо учитывать при формировании оперативно-следственной группы.

Как показывает практика, проведение осмотра места происшествия при проверке сообщений об установке и использовании *скиммера* вызывает особую сложность. Это обусловлено необходимостью правильно определить границы осмотра, круг участников следственного действия; многообразием производимых действий, направленных на обнаружение, изъятие, надлежащую упаковку предметов, имеющих значение для дела, и оставленных на месте совершения преступления следов, фиксацию и протоколирование производимых действий, соблюдение прав участвующих лиц.

УПК РФ (ст.ст. 176, 177, 180) регламентирует общие и обязательные требования, предъявляемые к процедуре проведения указанного следственного действия, которые необходимо учитывать при его осуществлении с целью придания в дальнейшем полученным результатам статуса доказательств, в то время как необходимая и достаточная в каждом случае совокупность действий, равно как и их последовательность, определяются следователем.

Поэтому ввиду сложности осмотра места происшествия применительно к выявлению и идентификации в банкомате внештатного оборудования, необходимо исходить из целого ряда практических рекомендаций, позволяющих правильно оценить обстановку.

Так, с целью обнаружения таких *скимминговых* устройств, как видеокамеры, накладки на клавиатуру, приспособления, считывающие магнитные полосы, а также следов их установки (клей, скотч и т. д.), иных предметов, имеющих значение для дела, следует произвести осмотр не только банкомата и непосредственно находящихся поблизости объектов, но и прилегающей территории.

Вблизи банкомата может находиться использованный преступниками автотранспорт с имеющими отношение к внештатному оборудованию техническими

устройствами (видеокамеры, накопители информации, ноутбуки, планшеты, флеш-карты, навигаторы, мобильные телефоны, сим-карты и т. д.).

В ходе осмотра места происшествия изымают записи камер видеонаблюдения.

Осмотр места происшествия производится в присутствии представителя банка, с участием специалиста. При отсутствии понятых закон предусматривает необходимость применения технических средств фиксации его хода и результатов (ч. 1^1 ст. 170 УПК РФ).

Однако в случаях осмотра места происшествия в рамках проверки сообщений об установке и использовании *скиммера* фото- и видеофиксация производимых действий представляется обязательной независимо от присутствия понятых, о чем участники следственного действия предупреждаются до начала его проведения, а сведения о применяемых технических средствах, об условиях и порядке их использования, об объектах, к которым они были применены, должны быть указаны в протоколе следственного действия (ст. 166 УПК РФ).

Банкомат, оборудование, имеющие отношение к делу другие предметы, автотранспорт проверяются на наличие следов рук, потожировых и иных следов, оставленных человеком, которые в случае их обнаружения должны быть изъяты, упакованы с указанием индивидуальных признаков, опечатаны и заверены подписью компетентного должностного лица на месте осмотра происшествия (ч. 3 ст. 177 УПК РФ).

Все подлежащие изъятию обнаруженные предметы предъявляются участникам следственного действия.

Значимыми для решения вопроса о возбуждении уголовного дела и последующего расследования являются сведения из банка, которому банкомат принадлежит. Данные сведения подтверждаются выписками из расчетных счетов пострадавших лиц и, соответственно, содержат информацию о хищениях денежных средств клиентов.

Из заявлений и объяснений граждан о хищении у них денежных средств могут быть установлены обстоятельства, имеющие решающее значение для решения вопроса о возбуждении уголовного дела, в том числе подтверждающие факт установки *скиммера,* незаконного получения сведений, составляющих банковскую тайну лица, и хищение его денежных средств, место и время совершения указанных действий.

В тех ситуациях, когда уголовное дело возбуждается в результате задержания лица при установке или снятии внештатного оборудования, следует учитывать значение выяснения обстоятельств его приобретения, использования, цели установления, выявления круга соучастников и видов соучастия, возможных мест нахождения причастных к преступлению лиц, адресов, телефонов, мест изготовления дубликатов карт, мест и времени передачи незаконно полученной информации, носителей ее содержащих для изготовления дубликатов карт.

После возбуждения уголовного дела в числе следственных действий приоритетное значение приобретает проведение обыска с целью обнаружения, например, дубликатов кредитных карт, оборудования, предназначенного для несанкционированного считывания информации с банковских карт или приспособленного для изготовления его элементов, компьютерной техники и т. д.

По общему правилу обыск в жилище проводится по судебному решению. Для этого следователь с согласия руководителя следственного органа выносит постановление о возбуждении перед судом ходатайства о производстве обыска.

Принимая во внимание, что при расследовании преступлений с использованием внештатного оборудования под подозрение в причастности к их совершению попадает достаточно широкий круг лиц, в каждом случае возбуждения соответствующего ходатайства надлежит обращать самое серьезное внимание на содержание *описательно-мотивировочной* части постановления, из содержания которой исчерпывающим образом должны усматриваться законность, обоснованность и необходимость проведения обыска у конкретного лица. Это позволит судье принять надлежащее решение без затребования дополнительных сведений и, соответственно, в кратчайшие сроки.

Однако в исключительных случаях проведение обыска допускается в порядке, предусмотренном ч. 5 ст. 165 УПК РФ, – по постановлению следователя с последующим уведомлением судьи и прокурора о его производстве. Здесь необходимо учитывать, что к уведомлению прилагаются копии постановления о производстве следственного действия и протокол следственного действия, что накладывает на должностных лиц обязанности как по надлежащему обоснованию законности и обоснованности его производства *без судебного решения, так и по надлежащему процессуальному оформлению его хода и результатов*. В противном случае все полученные в ходе такого следственного действия доказательства признаются недопустимыми в соответствии со ст. 75 УПК РФ.

Важным направлением деятельности следователя при расследовании преступлений, совершаемых с использованием скимминговых устройств, является назначение экспертиз, среди которых важное место занимают компьютерная, химическая, бухгалтерская, портретная, дактилоскопическая.

В соответствии с ч. 1 ст. 144 УПК РФ назначить судебную экспертизу и получить заключение эксперта можно до возбуждения уголовного дела, т. е. в ходе проверки сообщения о преступлении.

Однако следует учитывать, что перечень прав, указанных в ч. 1 ст. 198 УПК РФ, которыми наделены подозреваемый, потерпевший, свидетель при назначении и производстве судебной экспертизы, имеют под собой объективные основания *на этапе предварительного расследования*, т. е. применительно к конкретно определенному кругу лиц, наделенных соответствующим процессуальным статусом.

В то же время, до возбуждения уголовного дела они таким статусом не обладают. В связи с этим, а также исходя из целесообразности разглашения сведений, связанных с назначением соответствующих экспертиз лицам, не обладающим конкретно определенным процессуальным статусом, на данном этапе уголовного судопроизводства реализация совокупности прав, указанных в ч. 1 ст. 198 УПК РФ, представляется избыточной.

При этом следует подчеркнуть *необходимость соблюдения прав участников уголовного судопроизводства* для получения допустимых доказательств в результате проведения следственных действий, что, безусловно, надлежит учиты-

вать при решении вопроса о целесообразности назначения и производства судебной экспертизы на соответствующем этапе уголовного судопроизводства.

Помимо изложенного, надлежит обратить внимание на вопросы квалификации преступлений, совершенных с использованием автоматических терминалов самообслуживания, наиболее распространенными из которых, как показывает практика, на текущий момент являются *хищения* денежных средств по скомпрометированным банковским картам.

Вместе с тем необходимо учитывать, что хищению денежных средств из банкоматов путем установки и использования внештатного оборудования предшествует совокупность действий, направленных на незаконное получение (разглашение) сведений, составляющих коммерческую, налоговую или банковскую тайну соответствующего лица, указанных в ст. 183 УК РФ, предусматривающей уголовную ответственность за их собирание незаконным способом.

Поэтому действия лиц, получающих неправомерный доступ к охраняемой законом тайне – персональным данным владельцев банковских карт при помощи внештатного оборудования, следует квалифицировать по соответствующей части данной статьи.

Вместе с тем квалификация деяния может определяться моментом выявления преступления. Так, в случае задержания лица при установке или снятии скимминговых устройств уголовное дело возбуждается по ч. 3 ст. 30 (*покушение на преступление*) и соответствующей части ст. 183 УК РФ, а впоследствии, при установлении фактов, свидетельствующих о *совершении преступления*, привлечение в качестве обвиняемого предполагает квалификацию фактически осуществленных действий по ст. 183 УК РФ в той части, которой они соответствуют.

В тех случаях, когда после получения несанкционированного доступа к персональным данным владельцев персональных банковских карт с их счетов были похищены денежные средства, содеянное квалифицируют по совокупности ст.ст. 183 и 158 УК РФ.

При этом необходимо учитывать, что хищение денежных средств *из банкомата путем использования заранее похищенной или поддельной платежной* карты без участия уполномоченного работника кредитной организации следует квалифицировать как тайное хищение чужого имущества (кража) по соответствующей части ст. 158 УК РФ [4], т. е. разграничивать с мошенничеством.

Следует отметить, что в последнее время количество преступлений, связанных с хищениями из банковских автоматических терминалов самообслуживания с использованием внештатного оборудования несколько уменьшилось. Во-первых, банковское сообщество отреагировало на сложившуюся криминогенную ситуацию и установило оборудование с устройствами, которые выдают денежные средства только с карт, имеющих встроенные чипы, что значительно осложнило возможности «реализации» данных полученных с использованием скимминговых устройств. Во-вторых, нельзя не признать успешную деятельность правоохранительных органов по выявлению и расследованию преступлений, задержанию и привлечению к ответственности лиц, занимающихся созданием, установкой и использованием внештатного оборудования в преступных целях.

Вместе с тем, количество хищений по-прежнему остается значительным в ходе неправомерного использования реквизитов персонифицированных банковских карт, их ПИН-кодов, номеров и т. д., которые становятся известны преступникам, например, при оплате товара в сети Интернет, переводе денег с одного счета на другой.

Кроме того, в средствах массовой информации предупреждают о возможности использования в период проведения чемпионата мира по футболу банкоматов, приобретенных для скимминга на вторичном рынке, которые могут быть визуально замаскированы под банкоматы известных банков. Если клиент попытается снять деньги в таком банкомате, он получит сведения об ошибке, в то время как данные его банковской карты станут известны преступникам. При этом, поскольку данный банкомат фактически не будет принадлежать ни одной официальной банковской структуре, вопрос о возврате денет станет проблематичным [5].

Изложенное свидетельствует о необходимости постоянного расширения объема знаний, необходимых для совершенствования правоприменительной деятельности, что предполагает взаимообмен опытом с сотрудниками безопасности финансово-кредитных учреждений [6–9], в том числе и в ходе научных конференций, использование уже разработанных и разработка новых, соответствующих реалиям криминогенной обстановки в указанной сфере методических рекомендаций.

Список литературы

1. «Налоговый кодекс Российской Федерации, часть первая» от 31 июля 1998 г. № 146-ФЗ (ред. от 29.12.2017), ст. 102 // СПС «КонсультантПлюс». – URL: https://www.consultant.ru. – 2019.

2. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», ст. 3 // СПС «КонсультантПлюс». – URL: https://www.consultant.ru. – 2019.

3. Федеральный закон от 3 февраля 1996 г. № 17-ФЗ «О банках и банковской деятельности» (в ред. от 31.12.2017 № 482-ФЗ), ст. 26 // СПС «КонсультантПлюс». – URL: https://www.consultant.ru. – 2019.

4. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // URL: www.garant.ru.

5. Газета «Коммерсантъ». – 2018. – 29 янв.

6. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 134.

7. Мешков М. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / М. В. Мешков, В. В. Гончар // Мировой судья. – 2015. – № 4. – С. 14–18.

8. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

9. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Большунов Александр Геннадьевич[1]**,**
преподаватель кафедры специальных информационных технологий УНК ИТ Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ И БОРЬБЫ С ПРОЯВЛЕНИЯМИ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Правоохранительными органами Российской Федерации в январе – сентябре 2019 г. зарегистрированы 205,1 тыс. (+69,2 %) преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Сотрудниками органов внутренних дел задокументированы 201,7 тыс. (+70,3 %) IT-преступлений, при этом в массиве выявленных преступлений они составляют 14,2 % от общего числа преступлений, выявленных органами внутренних дел. Почти половина рассматриваемых преступлений – 97,4 тыс. (+174,1 %) – относится к тяжким и особо тяжким составам преступлений, раскрываемость которых составила 20,5 %.

Информационно-телекоммуникационное пространство является также основным средством коммуникации для экстремистских и террористических организаций. В январе – сентябре 2019 г. органами внутренних дел выявлены 185 (−73,1 %) криминальных деяний против общественной безопасности и государственной власти.

Распространение экстремистских материалов в форме статей, видеоматериалов, изображений, аудиозаписей, провоцирующих насилие в социальных сетях, сайтах, блогах и Telegram-каналах, становится главной темой в политике безопасности любого государства мира. Экстремисты активно используют информационные технологии с целью общения между собой, пропаганды экстремистских идей, организации сообществ и групп радикального направления.

Интернет является не только ключевым источником информации, он позволяет вести пропаганду без физического контакта. Конечно, он не заменяет личностного общения, он скорее дополняет его и действует как процесс идеологической обработки. Интернет действует как «эхо», которое позволяет человеку находить, прежде всего, поддержку своих идей, тем самым ускоряя процесс саморадикализации человека.

Информационные технологии представляют широкие возможности для анализа данных. Но природа вычислительной техники такова, что результаты ее работы с трудом воспринимаются человеком. На помощь приходят средства визуальной аналитики. Эти системы формируют графическое изображение ситуационного поля в виде схем, диаграмм, графовых конструкций. Переход от текстового или табличного представления к наглядному изображению повышает способность человека принимать решения на основе обработанных машиной данных. Одной из главных проблем в борьбе с экстремизмом являются социальные сети, они по-прежнему являются главной площадкой для поиска людей, подверженных влиянию и навязыванию идеологии экстремизма.

Социальная сеть (англ. *social networking service*) – платформа, онлайн-сервис или веб-сайт, предназначенная для построения, отражения и организации социальных взаимоотношений, визуализацией которых являются социальные графы.

Характерными особенностями социальной сети являются:

1. Предоставление практически полного спектра возможностей для обмена информацией (фото, видео, сервис блогов, сервис микроблогов, сообщества, личные сообщении, чат, возможность отметить местоположение и т. п).
2. Создание профилей, в которых требуется указать ФИО и максимальное количество информации о себе.
3. Подавляющее большинство друзей пользователя в социальной сети – это не виртуальные друзья по интересам, а реальные друзья, родственники, коллеги, одноклассники и одногруппники.

Сайт социальной сети можно определить по наличию следующих возможностей:

1. Создание публичного или непубличного профиля пользователя (например, профиль может содержать дату рождения, место обучения, хобби и многое другое).
2. Пользователь может задавать и поддерживать список других пользователей, с которыми у него имеются некоторые отношения (например, дружба, родство, деловые и рабочие связи и т. п.).
3. Просмотр и обход связей между пользователями внутри системы (например, пользователь может видеть друзей своих друзей).

Первое, с чего начиналось исследование, – это аккаунты пользователей. Социальные сети создаются для того, чтобы люди могли общаться между собой, вступать, создавать, объединяться в различные группы по различным тематикам, в которых они также ведут свое общение. Общение – это следующий аспект, который представляет интерес для изучения. Объектами в данном случае будут являться: посты и все, что появляется на стенах у пользователей, на стенах в группах. Все эти объекты представляют разную сущность, но их объединяет то, что у них есть свой набор определенных свойств или атрибутов, а свойства можно изучать и анализировать.

Свойства, которые можно выделить у всех этих объектов, – это все то, что пользователь указал про себя на своей странице: дата рождения, имя, фамилия, отчество, город, образование, интересы, военная служба и многое другое. У группы совсем другие параметры: название группы, на которую человек подписан, статус группы, подписчики, контактная информация.

Посты – это текстовая или медийная информация, заодно включающая в себя такие параметры, как отметки «мне нравится», «комментировать», а также информацию о количестве репостов – это основные объекты, которые присутствуют в социальной сети. Но на самом деле все эти объекты не представляют интереса для аналитического исследования, так как они нам изначально известны. Мы просто можем зайти на страницу интересующего нас объекта в веб-интерфейсе социальной сети и посмотреть эту информацию.

Группы тоже всегда представляют интерес для изучения связей, вся социальная сеть – это фактически связи между различными объектами. Пользовате-

ли дружат друг с другом, пользователи входят в группы, пользователи выкладывают посты на стене. Из всего этого многообразия графов можно выделить отдельные подструктуры, которые интересны для изучения.

Обычно при изучении графов социальной сети можно выделить несколько отдельных подклассов:

а) граф друзей, который показывает связи типа «Дружба» между пользователями, т. е. кто и с кем дружит в изучаемом сообществе;

б) граф участников групп, который показывает, какие пользователи входят в данную группу;

в) граф постов, который показывает посты на стенах пользователей или групп.

Именно изучение связей внутри графов позволяет проводить мощный глубинный анализ изучаемых объектов. Основная аналитика будет основана именно на изучении указанных графов: связи типа «Дружба», участников групп, постов на стенах. Но перед тем как переходить к основной части изучения, рассмотрим еще дополнительные вопросы, касающиеся способа классификации изучаемых групп.

Класс – это группа объектов с одинаковым набором характеристик, а классификация – это распределение объектов на классы и подклассы по основаниям классификации. То есть классификация подразумевает выделение некоторого общего признака, на основе которого мы производим выделение интересующих нас объектов из исходного множества. Классификация нужна для того, чтобы более точно концентрироваться на интересующих нас вопросах.

Например:

– отобрать для исследования все группы с открытым контекстом;

– отобрать для исследования все группы с малым и средним количеством участников (для оперативной обработки);

– отобрать все вновь созданные группы под какое-то конкретное мероприятие;

– отобрать все группы по интересующей нас тематике исследований (например, экстремизм, радикальный исламизм и т. д.).

После того как были определены объекты изучения в социальных сетях и проведена классификация групп, перейдем к основной части исследования. Весь этап исследования групп социальных сетей можно разбить на несколько последовательных шагов:

1. Формирование списка групп для исследования. Под списком групп можно понимать как одну отдельную взятую группу, так и набор групп. Таким образом, первый шаг – это выбор объектов для изучения.

2. Сбор данных для последующего анализа. Для того, чтобы иметь возможность произвести анализ, мы должны собрать определенный пласт информации.

3. Непосредственный анализ собранной информации.

Теперь рассмотрим все эти шаги более детально.

Первый шаг в проведении исследований – это формирование списка групп для исследований. На этом шаге мы должны неким образом задать интересующие нас группы.

Можно выделить два основных направления в формировании такого списка:

1. Готовый список. Например, мы можем получить такой список от коллег по отделу, от руководства, из внутренней системы учета групп и т. д. Фактически, нам надо задать список ссылок на изучаемые группы в любом удобном для нас формате.

2. Сбор информации. На выходе первого шага у нас есть список групп для исследования. На данном этапе мы переходим от заданного списка групп к формированию отдельных объектов для их последующего детального анализа. Данный шаг служит дополнительной проверкой корректности входного списка групп (например, список групп мог быть сформирован давно, и отдельные группы из этого списка могли быть уже закрыты).

После того как мы провели предварительный сбор информации, мы переходим к основному этапу – анализу.

3. Анализ групп путем исследования связей с другими объектами. Данный этап подразумевает сбор дополнительной вспомогательной информации в рамках интересующих исследований и затем – дальнейший анализ этой информации.

Всего можно выделить три основных направления по анализу групп:

- сбор и анализ информации об участниках групп;
- сбор и анализ информации постов участников групп;
- различная дополнительная аналитика.

Первый шаг анализа – сбор и анализ статистической информации об участниках; этот шаг еще называют «атрибутным анализом».

Какая статистическая информация по участникам групп интересна для анализа?

Первый очень важный шаг анализа – анализ так называемых мертвых ссылок. Это подразумевает, что на странице каждой группы указано количество участников этой группы. Очень часто бывает так, что во время сбора реальных данных количество собранных участников может быть намного меньше заявленного на странице группы. Очень часто аккаунты участников групп блокируются (закрываются) самой социальной сетью в силу противоправных действий со стороны этих участников (оскорбительные надписи в постах, распространение запрещенных медиаматериалов, жалобы со стороны других пользователей и т. д.).

Таким образом, процент «мертвых» ссылок участников группы может косвенно показывать на экстремизм группы (чем больше процент «мертвых» ссылок, тем выше степень экстремизма участников).

Следующий интересный параметр анализа – гендерное соотношение участников (процентное распределение по полам). Как показывает практика, обычно группы экстремистских тематик, состоящие в основном из мужчин, более склонны к агрессивным действиям, чем группы с равномерным распределением полов.

Дальше можно анализировать любые другие интересующие нас параметры. Например, распределение участников по городам. Такая информация может быть полезна при прогнозировании событий в определенном городе во время определенных мероприятий.

Анализ дат рождения участников группы позволяет составить картину о возрастном распределении. Можно использовать статистический анализ для оценки любых интересующих нас параметров в рамках решаемых задач:

- образование участников;
- место работы;
- прохождение военной службы и т. д.

После проведения статистического анализа можно переходить к более глубокому изучению групп на основе дополнительного анализа связей.

Первое направление анализа связей: поиск лидеров по количеству общих групп. Например, поиск лидеров по количеству связей с другими участниками. Помимо метрики «Степень» (количество связей с другими объектами в графе) существуют и другие метрики, которые помогают искать лидеров по различным параметрам лидерства (промежуточность, близость, собственный вектор и т. д.). Выбор метрики центральности для поиска лидеров зависит от решаемых задач.

Другое важное направление в исследовании связей участников – поиск кластеров (или групп наиболее тесно связанных между собой участников). Фактически, это обозначает поиск скрытых подсообществ внутри исследуемых групп. После того как мы нашли кластеры, мы можем продолжить исследование отдельных интересующих нас кластеров на предмет понимания, за счет чего именно возникли эти кластеры.

Выделив нужный нам кластер для исследования, мы можем попытаться понять, что общего у данных членов кластера (образование, работа, совместная служба в армии и т. д. Найдя совпадения по атрибутам, мы можем понять причину возникновения таких кластеров. Все это относится к первому направлению исследования групп (исследование групп через анализ участников).

Посты – это та информация, которая помещается на стене группы. Тут можно провести различные виды анализа, начиная от статистического анализа (по аналогии со статистическим анализом участников групп), т. е. когда мы проводим статистический анализ всей доступной атрибутной информации постов, переходя к временному анализу. Такой вид анализа возможен в силу того, что посты содержат дату размещения. За счет этого можно получать очень много интересных временных оценок.

Далее – анализ связей. Подразумевается всевозможный анализ связей постов с другими объектами социальной сети.

Заключительный этап – анализ содержимого постов. Это подразумевает и синтаксический разбор содержимого текстов, и анализ медиаконтента, и получение ссылок на другие интернет-ресурсы.

Дополнительная аналитика подразумевает все те виды анализа, которые не входят в первые два направления исследований. Первый пример: мониторинг изменений групп за заданный период времени. Это подразумевает сравнение интересующих нас характеристик в разные периоды времени:

- получение списка новых участников за заданный период;
- получение списка новых постов за заданный период;
- получение новых реакций на посты (лайки, репосты, комментарии).

Другой пример: поиск смежных групп или поиск групп со схожей тематикой. Когда мы исследуем список группы по заданной тематике, мы не можем быть полностью уверены, что мы охватили для исследования все группы данной тематики. Имена групп могут быть неочевидны: группы могут шифроваться намеренно.

Одна из очень важных задач анализа – найти группы схожей экстремисткой тематики. Обычно это делается путем задания некоторого процентного порога. И если участники нашей известной группы массово входят в другую неизвестную нам группу, причем процент вхождения больше или равен заданному порогу, то мы можем считать, что потенциально нашли группу, схожую по интересам с нашей заданной.

Подводя итог, мы можем сказать, что были рассмотрены основные этапы исследования групп социальных сетей экстремистского характера. Напомню, что в качестве этих этапов можно выделить следующие шаги:

- выбор объектов исследования;
- сбор данных;
- проведение аналитики на собранных данных.

Статистический анализ групп позволяет оценить следующие параметры:

- потенциальный уровень экстремизма;
- активность группы;
- дополнительная оценка интересующих параметров участников (город, средний возраст, образование и т. д.).

Анализ связей позволяет найти следующие интересные объекты для последующего детального изучения:

- лидеров по различным критериям значимости;
- смежные группы по схожей тематике.

Дополнительно может присутствовать возможность управления содержимым в рамках своего профиля, образование групп пользователей с различными режимами членства, возможности веб-синдикации, использование приложений и многое другое. С точки зрения информационного обеспечения деятельности правоохранительных органов наибольшее значение имеет деление информационных ресурсов по категории доступа на общедоступные (открытые) и с ограниченным доступом.

Серезевский Алексей Вадимович[1]***,***
заместитель начальника кафедры
специальных информационных технологий УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ DLP-СИСТЕМ В ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время широкое распространение получили системы защиты от утечки конфиденциальной информации, так называемые DLP-системы.

Основным предназначением такого рода систем является то, что они в режиме реального времени позволяют отслеживать и, в случае возможной утечки конфиденциальной информации, блокировать входящие и исходящие сообщения сотрудников, копирование файлов на внешние носители, сетевые информационные и облачные хранилища, веб-ресурсы. Современные DLP-системы настолько функциональны, что позволяют управлять не только текстовыми, но и голосовыми сообщениями, передаваемыми во внешнюю среду посредством протокола *SIP* (IP-телефония, видео- и аудиоконференции, мгновенные сообщения), с целью предотвращения утечки информации, распространение которой может нанести тот или иной ущерб.

DLP-системы представляют собой программный продукт, который устанавливается в локальной сети организации и может анализировать потоки данных на границе защищаемого периметра или на рабочих станциях пользователей и, в зависимости от настроенных параметров, выполняет блокировку несанкционированных информационных потоков. Также такие системы обладают возможностью записи копии внешнего трафика для последующего анализа в случае расследования возможной утечки.

DLP-системы защиты от утечек конфиденциальной информации предназначены для решения следующих задач:

– хранение копий конфиденциальной информации, передаваемой посредством электронной почты, мессенджеров и IP-телефонии, а также пересылаемой на внешние носители и сетевые корпоративные, а также веб-ресурсы, с целью дальнейшего расследования инцидентов утечки конфиденциальной информации;

– блокирование передачи конфиденциальной и другой информации ограниченного пользования за пределы организации;

– блокирование передачи ненадлежащей информации во внутреннюю сеть организации;

– блокирование возможности сотрудников использовать ресурсы организации в личных целях;

– поиск мест нахождения несанкционированных копий конфиденциальной информации;

– управление действиями сотрудников (контроль присутствия на рабочем месте, отслеживания их лояльности и надежности и т. п.).

DLP-системы защиты от утечек конфиденциальной информации включают в себя следующие подсистемы:

1. Сетевая подсистема, располагающаяся в граничной с внешним миром части сети. Если установлена система *DLP*, то весь трафик организации проходит через такую систему, и она анализирует его в соответствии с настроенными правилами и политиками. В случае, когда риски компании при отправке заблокированного сообщения достаточно велики, DLP-системы не устанавливаются в сети, а передают трафик на нее с прокси-сервера или почтового сервера. Таким образом, администраторы безопасности всегда смогут просматривать архивы сообщений и инцидентов, записанных системой.

2. Подсистема контроля рабочих станций. Она обычно устанавливается непосредственно на все компьютеры сотрудников компании. Учитывая, что установка может быть выполнена удаленно, пользователи могут не знать, что их действия отслеживаются. Однако при использовании функции блокировки передачи данных DLP-системы могут отображать окно сообщения об ошибке, если нарушаются политики. Подсистема контроля рабочих станций может контролировать копирование информации в буфер обмена, передачу данных по электронной почте, различные мессенджеры, отправку данных на внешние носители, а также отправку файлов и данных по протоколу *HTTPS* (например, в облачное хранилище). Важной особенностью здесь является возможность анализа данных непосредственно перед их отправкой по зашифрованному каналу связи, что в ряде случаев является единственной возможностью их перехвата.

3. Центральный блок управления. Для того, чтобы качественно настроить DLP-систему, даже при должном уровне подготовки и наличии опыта необходимо потратить много времени и проанализировать много информации. Современные системы защиты от утечек позволяют использовать предустановленные словари для настройки фильтрации контента. Такие словари могут содержать списки профессиональных терминов различной тематики (для отдела кадров, отдела информационной безопасности, различных финансовых и юридических терминов), списки слов с нежелательными выражениями, а также регулярные выражения для таких данных, как номера документов, удостоверяющих личность или банковских карт.

Эксперты отмечают, что в настоящее время проявляется четкая тенденция перехода от «латаных систем», состоящих из компонентов защиты информации различных производителей и решающих отдельные задачи, к единому комплексу программ. Сложные интегрированные системы избавляют специалистов по информационной безопасности от необходимости решать проблемы совместимости различных компонентов. Такие DLP-системы также позволяют IT-специалистам удобно изменять настройки на большом количестве клиентских рабочих станций и оптимизировать передачу данных от одного компонента единой интегрированной системы к другому. Разработчики также переходят на интегрированные системы в связи со спецификой задач информационной безопасности. Если хотя бы

один канал утечки информации в организации остается незащищенным, нельзя в целом говорить о какой-либо защите вообще.

Еще одной важной тенденцией современных DLP-систем является постепенный переход к модульной структуре. Это означает, что клиент может выбрать необходимые компоненты (например, если поддержка внешних устройств отключена на уровне операционной системы, клиенту не нужно платить за их управление).

Следует также отметить, что отраслевая специфика играет значительную роль в развитии DLP-систем. Существуют специальные версии, разработанные специально для банковского сектора, государственных органов и т. д., которые удовлетворяют потребности данных организаций с учетом специфики их деятельности.

В связи с изложенным внедрение DLP-систем в деятельность органов внутренних дел представляется достаточно целесообразным. Поскольку многообразие представленных на рынке таких систем достаточно велико и специфика деятельности органов внутренних дел требует особого подхода при их выборе и внедрении, необходимо сформулировать технические требования к специализированной версии DLP-системы для подразделений органов внутренних дел. Данные мероприятия целесообразно проводить в рамках научно-исследовательской работы с привлечением широкого круга специалистов.

Овчинский Анатолий Семенович[1]**,**
профессор кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

Борзунов Константин Константинович[2]**,**
доцент кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник

ПЕРСПЕКТИВЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ МИРЕ

Автоматизированная обработка данных и сведений, составляющих ресурсы оперативно-разыскной информации вместе с сигналами и потоками данных, как циркулирующих в сети Интернет, так и получаемых с десятков тысяч камер видеонаблюдения, открывает новые возможности в повышении эффективности информационно-аналитического обеспечения правоохранительной деятельности.

Оперативно-разыскную информацию в методологическом плане можно представить в единстве:

– *реактивной* оперативно-разыскной информации, которая, являясь целью ОРД, необходима для планирования и осуществления оперативно-разыскных мероприятий;

– *ресурсной* оперативно-разыскной информации, которая, представляя базу ОРД, включает структурированные данные и сведения оперативно-разыскного назначения наряду с накопленными оперативно-разыскными знаниями;

– *фоновой* оперативно-разыскной информации, которая, выступая виртуальной средой ОРД, циркулирует в пространстве социальных коммуникаций и сетевом эфире, накапливается на интернет-платформах, содержит сведения, необходимые для решения оперативно-разыскных задач.

В развитии технологий и методов информационно-аналитической работы в ряде случаев представляется целесообразным выделить суть как базового информационного, так и собственно аналитического обеспечения мер по профилактике, раскрытию и расследованию преступлений.

Информационное обеспечение правоохранительной деятельности состоит: в накоплении необходимых учетных, регистрационных и биометрических данных; в совершенствовании ресурсов оперативно-разыскной информации; в создании единого структурированного информационного пространства, охватывающего субъекты ОРД во всех регионах страны.

Аналитическое обеспечение профилактики и раскрытия преступлений в цифровом мире заключается: в разработке и применении алгоритмов автоматизированной обработки поступающих и накопленных данных и сведений; в получении реактивной оперативно-разыскной информации, позволяющей

адекватно реагировать на развитие криминальной ситуации, предотвращать и раскрывать преступления; в накоплении потенциалов социально-психологической энергии, позволяющей эффективно осуществлять меры по борьбе с преступностью и обеспечению общественной безопасности.

Непосредственно аналитическая работа должна опираться на такие технологии получения, обработки и анализа данных, которые обусловлены: развитием сетевых коммуникаций с множеством как доступных, так и скрытых интернет-платформ; вступлением в «цифровой мир» с «Интернетом всего» – средств связи и контроля, технологическими линиями и бытовыми приборами, датчиками и имплантами; внедрением систем искусственного интеллекта с возрастающими возможностями распознавания и гибкими алгоритмами обучения и самообучения нейронных сетей.

Важно представлять, что базу и среду оперативно-разыскной аналитики будущего составят Большие данные. С позиции реактивных, ресурсных и фоновых представлений об информации [1] они вбирают в себя:

– ресурсы структурированной информации, банки данных субъектов оперативно-разыскной деятельности, государственных учреждений, коммерческих и финансовых предприятий, общественных фондов и организаций;

– фоновую неструктурированную информацию, потоки сообщений сетевого эфира и средств массовой информации, содержание сайтов, блогов, электронной переписки, результаты видеонаблюдения, аудиоконтроля, фиксации разнообразных параметров;

– реактивную информацию с автоматическим реагированием и принятием решений самообучающимися нейронными сетями на основе гибких перенастраивающихся алгоритмов использования систем искусственного интеллекта.

Среди перспективных направлений информационно-аналитического обеспечения правоохранительной деятельности можно выделить экспресс-аналитику, инициативную аналитику, ретроспективную аналитику, предиктивную аналитику, актуальную аналитику, глобальную аналитику.

Экспресс-аналитика направлена на раскрытие преступлений «не отходя от компьютера». Лица, подозреваемые в совершении преступления, устанавливаются на основе данных камер видеонаблюдения и фотоизображений, имеющихся в базах данных оперативно-разыскных ресурсов.

Сведения из различных интернет-сегментов формируются в криминальные профили подозреваемых, устанавливаются их связи и возможные места нахождения. Использование данных о приобретенных билетах на авиа- и железнодорожный транспорт дает возможность организовать задержание выявленных вероятных преступников.

Инициативная аналитика стирает противоречие между непрерывным пополнением информационных оперативно-разыскных ресурсов и эпизодическим обращением к ним. Она направлена на превентивное выявление лиц, представляющих потенциальные угрозы общественному порядку и безопасности, требующих мер оперативно-разыскной профилактики. Такая аналитика показала свою эффективность при обеспечении безопасности Олимпийских и Параолимпийских игр (Сочи-2014), других массовых международных мероприятий, вклю-

чая Чемпионат мира по футболу 2018 г., который проходил в десяти городах России. Она перспективна при целенаправленных территориальных исследованиях контингента лиц, от которых можно ожидать преступлений и правонарушений в городах и населенных пунктах с повышенной криминогенной обстановкой.

Ретроспективная аналитика направлена на раскрытие преступлений прошлых лет, розыск пропавших лиц, установление неопознанных погибших. Она должна опираться на специально организованные матричные информационные ресурсы, содержащие пустые элементы для недостающих сведений, включает алгоритмы автоматического поиска данных и наполнение пустых элементов матрицы сведениями, требующимися для раскрытия преступлений прошлых лет.

Предиктивная аналитика направлена на профилактику преступлений, правонарушений и антисоциальных явлений. Это требует автоматизированных алгоритмов обращения к ресурсам оперативно-разыскной информации, использования нейросетей для обработки агентурных сообщений, оперативных сводок, Больших данных – фоновой информации, циркулирующей в сетевом эфире и социальных коммуникациях.

Фундаментальной теоретической базой применения предиктивной аналитики в профилактике преступлений является доказанное криминологическими исследованиями положение о том, что «нарастание незначительных отступлений от позитивного (в социальном и нравственном смысле) поведения может приводить человека к антиобщественным и общественно опасным поступкам».

Актуальная аналитика включает оперативно-криминологическое прогнозирование условий, обстоятельств, места, времени, заказчиков и исполнителей преступлений; применение алгоритмов обработки накопленных и поступающих данных вместе с разработкой и использованием комплекса криминологических моделей; «выход» на возможного исполнителя или заказчика преступления с ориентировкой на его личностные и физические качества, вплоть до внешнего вида, особенностей характера и поведения.

Глобальная аналитика направлена на выявление криминальных, террористических и экстремистских угроз. Она включает сбор и обработку данных из всех доступных каналов коммуникаций, обо всех регистрируемых событиях, касающихся всех людей.

Блоки информации о людях и событиях из разнородных баз данных и информационно-поисковых систем (ресурсная информация), наряду с информацией из процессинговых центров, транспортных компаний, федеральных и муниципальных органов и служб (фоновая информация), проходят обработку, например, на предмет выявления таких последовательностей разнородных и одновременно взаимосвязанных событий, вероятность которых подозрительно мала.

Информационно-аналитическое обеспечение правоохранительной деятельности в цифровом мире требует создания инфраструктуры, должно включать наряду со специализированными аналитическими подразделениями, факультетами подготовки специалистов, владеющими технологиями получения, обработки и анализа данных, центры накопления данных (информационных

ресурсов оперативно-разыскного назначения); центры разработки алгоритмов (автоматизированного поиска, обработки и анализа данных, криминологического прогнозирования, применения самообучающихся нейронных сетей, систем искусственного интеллекта); центры управления реактивной оперативно-разыскной информацией (об объектах, представляющих угрозу безопасности, требующих оперативного контроля и мер профилактических воздействий).

Список литературы

1. Овчинский А. С. Информационные координаты: Управление. Противоборство. Безопасность / А. С. Овчинский, К. К. Борзунов, С. О. Чеботарева. – М. : Горячая линия. – Телеком, 2018. – 270 с.

Ивлев Максим Иванович[1]**,**
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Плотников Герман Геннадьевич[2]**,**
профессор кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

К ВОПРОСУ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последнее время количество киберугроз возросло в десятки раз, а киберпреступники уже не являются хакерами-одиночками, как 10–15 лет назад, а представляют собой мощные группировки хорошо организованного и технически оснащенного криминала с многомиллионными оборотами денежных средств. Очень тревожной выглядит статистика инцидентов информационной безопасности (ИБ), которая собирается в банках и крупных компаниях, и это несмотря на то, что в корпоративном секторе работают службы ИБ, которые вооружены программно-техническими средствами в области защиты информации (*SIEM*, *DLP*, антивирусным программным обеспечением (ПО) и т. д.). Почему же, несмотря на такую приличную организацию защиты информационных активов в компаниях, все равно происходят инциденты ИБ с крупным ущербом? Специалисты по информационной безопасности давно осознали, что необходимы комплексный подход в сфере реагирования и расследования инцидентов ИБ и единое централизованное решение.

Защита информационных систем выходит на первое место практически в любой индустрии. Любой несанкционированный доступ к информации может привести к серьезным проблемам.

Информационная система любой, даже самой маленькой компании, сложносоставная, и все ее части должны защищаться по одному и тому же принципу: сначала организационные, затем превентивные меры, потом средства наблюдения, детектирующие аномалии и инструменты реагирования. На последнем по порядку, но не по значимости этапе борьбы с угрозами стоят люди, хотя случается, что проблему безопасности можно решить не привлекая людей, например путем автоматической блокировки портов или отключения от общей сети. Инструменты, используемые для защиты каждого из компонентов системы, могут быть разными, но прослеживается общая тенденция прихода к идее внедрения *SOC – Security Operation Center*.

SOC – это инфраструктура с множеством взаимосвязанных компонентов, его основа – *SIEM* (*Security information and event management*). *SIEM* – это система сбора, нормализации и корреляции данных, которая собирает логи с вебсерверов, хостовых машин и других инфраструктурных компонентов, а также со

средств защиты информации, установленных на устройствах сети организации, коррелирует и обрабатывает их, чтобы привести в нормализованный вид. Это и есть основная задача *SIEM* – привести к единому формату огромное количество логов от разных источников для удобства обнаружения взаимосвязей между ними. Это нужно для еще одной составляющей *SOC* – аналитиков *SOC*, которые, глядя на огромные списки логов из *SIEM*, должны на какие-то из событий реагировать самостоятельно или же передавать их в работу специалистам по безопасности.

Центры мониторинга и реагирования на инциденты (англ. *Security Operations Center – SOC*) появились не так давно как средство информационной безопасности. Это инструмент для обеспечения целостного и комплексного подхода в вопросе мониторинга и реагирования на инциденты, согласно нормативным документам регулирующим ИБ. *SOC* является единой платформой для сбора, хранения и обработки информации о состоянии безопасности ИТ-инфраструктуры, уязвимостях и инцидентах ИБ.

Перед тем, как разворачивать в компании *SOC*, необходимо обозначить основные цели управления инцидентами ИБ. Таковыми, как правило, являются:

– обеспечение непрерывного процесса выявления любых событий, которые способны повлиять на безопасность организации;
– обеспечение адекватной реакции на произошедшие события;
– быстрое устранение последствий инцидента;
– извлечение полезных уроков из инцидентов и предотвращение их повторения в дальнейшем.

Далее рассмотрим основные задачи, которые должен решать *SOC*:

– инвентаризация и контроль инфраструктуры;
– консолидация информации об инцидентах ИБ;
– координация и автоматизация реагирования на инциденты ИБ;
– интеграция и получение данных из внешних источников;
– сбор показателей эффективности системы защиты (метрик).

На базе центров *SOC* довольно часто обеспечивается решение актуальных для каждой компании задачи по управлению информационными активами, таких как:

– мониторинг ИТ-инфраструктуры, сбор данных об оборудовании и его характеристиках (инвентаризация), контроль состава ИТ-систем, построение связей взаимодействия между компонентами;
– составление перечня критических активов и проведение оценки их ценности;
– контроль учетных записей пользователей, управление доступами и привилегиями;
– управление уязвимостями.

За счет соответствующих инструментов *SOC* выявляются наиболее критичные активы и определяются ответственные за эти активы специалисты. Все это осуществляется в тесном взаимодействии с другими инфраструктурными системами (антивирусами, сканерами уязвимостей и т. д.). Также, как правило, в рамках кон-

троля инфраструктуры осуществляется контроль за вновь установленными программами, выявляется ПО, которое не разрешено к использованию, фиксируется подключение нового оборудования и другие потенциально опасные активности. Визуализация данных по активам представляется в виде графов, схем, карт сетей, позволяющих повысить эффективность анализа защищаемой инфраструктуры.

Список литературы

1. Орехов П. В. Постановка и решение задачи нахождения криминального тренда связей / Е. Г. Белоглазов, П. В. Орехов // Математические проблемы информационной безопасности: сборник научных статей Всероссийского семинара. – М. : Московский университет МВД России имени В.Я. Кикотя, 2018. – С. 24–26.

Овчинский Анатолий Семенович[1]**,**
профессор кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

Борзунов Константин Константинович[2]**,**
доцент кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ В БОРЬБЕ С СОЦИАЛЬНОЙ ДЕСТРУКЦИЕЙ В ЦИФРОВОМ МИРЕ

В западной социологии весьма модным стало понятие информационной перегрузки как «состояния цивилизации, при котором объем потенциально полезной и актуальной информации превышает возможности ее обработки человеком» [1]. На самом же деле глобальные разрушительные последствия информационной войны связаны с внешне стихийной, но вполне последовательной и управляемой хаотизацией информационного фона, на котором формируется сознание новых поколений.

Несложно представить, что наряду с географическими, экономическими, социальными факторами именно информационная среда определяла те необходимые условия, в которых происходила консолидация племен, сообществ, народов. Формировались культурные традиции и устои, религиозные представления, мировоззренческие доктрины и идеологии, которые наполняли жизнь людей определенными смыслами.

Не будет большим преувеличением утверждение о том, что сегодня лавины сведений и сообщений часто просто сметают традиционные представления, а иногда и разрушают общепринятые смыслы жизни.

Активно обсуждая последствия информационного взрыва, западные философы, как правило, приходят к утверждению: «Информация не нуждается в том, чтобы ее воспринимали, не нуждается в том, чтоб ее понимали, она не требует умственных усилий для своей интерпретации, ей не требуется иметь смысл» [2].

Здесь как раз и заложено большое лукавство. Скрывается то обстоятельство, что потоки информации все в большей мере используются для контроля ситуаций и воздействий на людей, как в достижении меркантильных, локальных, коммерческих целей, так и в реализации стратегических устремлений по управлению мировыми процессами.

В научном и методологическом планах проблема заключается в том, что представления об информации развивались по весьма разнообразным траекториям. На условно гуманитарном пути информацию связывали с новыми знаниями, с сенсационными сообщениями. В кибернетике она представала в управляющих сигналах. Она проходила этапы формализации в математических моделях, обо-

гащала вычислениями теории связи и управления. В философии выделялись атрибутивный и функциональный подходы к информации.

Однако сейчас встретить результаты фундаментальных исследований природы собственно информации не удается. Аналогично, когда создавалась атомная бомба, исчезли работы по ядерной физике. В то же время, если применение ядерного оружия не требует углубления в суть нейронно-протонных взаимодействий, то успехи или неудачи операций информационной войны, как и эффективность информационного противоборства, напрямую связаны с сущностными проявлениями самой информации.

«Увидеть» возникновение и проявление собственно информации можно в реакциях на воздействия и побуждения. Реакции присущи всем объектам живой природы, а сейчас и роботизированным системам. В сознании человека реактивная информация возникает как функция целевой интерпретации поступающих сообщений и сигналов. И если в природных и технических системах роль информации состоит в обеспечении адекватных реакций, то сознанию человека именно реактивная информация позволяет понимать смысл происходящего, быть личностью, ощущать связь с прошлым, планировать будущее, иметь представление о том, что находится за пределами нашей реальности.

В отличие от реактивной, ресурсная информация фиксируется, накапливается и транслируется на определенных носителях. В живой природе это осуществляется физико-химическими и биологическими взаимодействиями. Истинно биологическая ресурсная информация, закрепленная в генетических кодах, в строении органов и тканей и передаваемая от вида к виду из поколения в поколение обеспечивает эволюцию жизни.

Социальная ресурсная информация требует внешних искусственных, уже созданных человеком носителей. Информационные технологии сегодня коренным образом меняют весь уклад жизни людей. Но и в прежние времена основные этапы в развитии цивилизации были связаны с методами и средствами получения и использования социальной ресурсной информации. Наскальные рисунки, петроглифы, иероглифы, алфавитная письменность, бумажные носители, книгопечатание, массовые издания, фото и киноизображение, радио и телевидение, электронные носители и сеть Интернет – это технологии фиксации, накопления и трансляции социальной ресурсной информации.

Наконец, фоновая информация непосредственно отражает окружающую реальность. Так же как реактивная и ресурсная, фоновая информация выступает атрибутом мироздания, проявляя фундаментальное свойство – отражение и создавая собственно фон как природной, так и социальной жизни. Она выполняет и свою функциональную роль, скажем, воздействуя на людей часто в обход защитных механизмов сознания.

Если реактивная информация позволяет выживать объектам природы, обеспечивая адекватность реакции, а людям понимать смыслы происходящего, ресурсная информация фиксирует и передает опыт выживания и развития, то фоновая информация включает механизмы адаптации к изменяющимся условиям обитания или социального окружения [3].

Важно, что представление информации в триединстве реактивных, ресурсных и фоновых проявлений, отражающих ее сущностные качества, дает еще и новую универсальную систему координат, в которой в трехмерном пространстве раскрываются самые разнообразные понятия, поскольку все явления и процессы нашей жизни и деятельности так или иначе построены на информационных взаимодействиях. Более того, фрактальный характер информационных координат позволяет проводить анализ с разной степенью детализации и переходами из одних областей знаний в другие.

В трехмерном пространстве информационных координат информационную войну против России, которая десятилетиями ведется западными странами, можно представить в единстве психоисторической, психоидеологической и психодемографической войны.

Идеи психодемографической войны восходят от мальтузианства и социодарвинизма. Они оформились в недрах Британской империи, прошли апробацию как на многочисленных колонизированных народах, так и на беднейших слоях населения самой Англии. Непосредственным уничтожением миллионов людей свой след в истории оставили фашистская Германия и милитаристская Япония. В последние, условно мирные десятилетия, на сокращение населения стран и регионов были направлены волны сексуальных революций, разрушения семейных ценностей, движения за права сексуальных меньшинств.

Заметим, что если в планах Адольфа Гитлера после победы в войне с Советским Союзом было оставить в живых не более 50 млн русских рабов, то Маргарет Тетчер после разрушения Советского Союза уже в преддверье новой промышленной революции заявляла, что в России достаточно иметь только 15 млн жителей для обслуживания нефтепромыслов, газопроводов и добывающей промышленности. И в «лихие» 1990-е гг. под ударами психодемографической войны население нашей страны ежегодно сокращалось на 600–700 тысяч человек.

Информационная война на разных уровнях общественного сознания велась и ведется и на идеологических фронтах. Идеологию необходимо рассматривать не столько как систему взглядов, отражающих отношение к окружающей действительности, сколько как глобальную мотивационную матрицу, обосновывающую право на те или иные действия и поступки, на образ жизни и мыслей.

Угрозы социальной деструкции вызревают с криминальной идеологией, идеологиями экстремизма и терроризма, обосновывающими право на преступную деятельность, на убийства и самоубийства, на разрушение основ государственности [5].

Возрастающие в виртуальном пространстве сетей, блогов, сайтов информационные потоки наполняются зловещими смыслами. Огромный спектр информационных ресурсов: от отечественных криминальных сообществ до американских расистских и неонацистских групп ненависти, от политических радикалов и протестных сообществ до уличных бойцов, от сайтов террористических организаций до виртуальных сект (неоязыческих, религиозных, сатанинских, тоталитарных, коммерческих) разрушает сознание многих миллионов людей, побуждая их к противоправным, асоциальным действиям, все чаще приводя к кровавым инцидентам с массовыми убийствами в самых разных местах планеты [6].

Можно по-разному оценивать роль и значение идеологии, но применив систему информационных координат, увидим, что реально борьба за сознание людей в современном мире ведется в пространстве трех основных мировых идеологии: либерализма, консерватизма и социализма.

При этом реактивный вектор – либерализм, агрессивно провозглашая приоритетность прав человека, настойчиво формирует человека-потребителя, человека мобильного (у которого Родина там, где лучше) и уже человека бесполого (сам выберет себе пол, когда подрастет).

Ресурсный вектор мировых идеологий – консерватизм, негативно воспринимаемый сторонниками прогресса, который, однако, возвращает нас к человеку-защитнику, человеку долга, человеку – патриоту своего отечества, ценящему духовные традиции своего народа.

Наконец, фоновый вектор – социализм, а в перспективе и коммунизм, незаслуженно снятый с пьедестала в нашей стране, отдавая приоритеты коллективизму и справедливости, напоминает, что высшее призвание человека заключается в творчестве, а смысл общественного развития – в формировании личности и раскрытии ее потенциала.

Если операции психодемографической и психоидеологической войн, как правило, имеют скрытый характер, то наиболее «горячие» информационные сражения сегодня происходят на психоисторическом фронте.

Ресурсный вектор истории в информационных координатах – это дошедшие до нас свидетельства, документы, артефакты, воспоминания очевидцев. Однако построение истории требует определенной интерпретации прошлого (это уже реактивный вектор построения истории). Но интерпретация отражает позицию исследователя, можно даже сказать, преследует определенные цели (здесь включается фоновый вектор истории, который, как правило, определяется идеологией, а часто и непосредственно стоящими задачами).

Если мыслители прошлого замечали, что история – это факел, высвечивающий будущее, то практика уже информационной эпохи показывает, что для изменения вектора развития страны меняют ее историю.

Информационные координаты отражают и уровни психоисторической войны: фактологический (фальсификация фактов), концептуальный (заданная интерпретация), метафизический (разрушение смыслов).

Одна из основных задач психоисторической войны состоит в том, чтобы скрыть субъекты глобального управления и истинные причины мировых потрясений. Сегодня именно Россия является эпицентром психоисторической войны как непреодолимый барьер к мировому господству. При этом главной мишенью информационных атак стала Победа в Великой Отечественной войне [7], хотя основные угрозы психоисторической войны состоят в отсутствии единого консолидированного подхода к построению своей героической истории.

Активное наступательное информационное противоборство должно включать создание и распространение такого тематического контента, который требуется для накопления позитивного потенциала социально-психологической энергии. Одновременно необходимы профилактические оперативно-разыскные, разведывательные и контрразведывательные мероприятия по выявлению ин-

формационных угроз и их источников. Наконец, требуется осуществление целенаправленных коммуникаций, формирующих сигналы для управления энергоинформационным потенциалом.

Намечая глобальные стратегии, которые должны быть взяты на вооружение в борьбе с внешними и внутренними деструктивными силами, следует обратиться к основным концептуальным приоритетам в управлении социальными процессами и международными отношениями [8].

Если ранее сложились и продолжают господствовать такие приоритеты, как военно-силовой, финансово-экономический и рефлекторно-психологический, то сейчас становится все более очевидным, что активные наступательные действия в информационном пространстве должны опираться в первую очередь на свою осмысленную и развивающуюся систему приоритетов.

Такими высшими приоритетами управления общественным развитием должны стать идеологический, исторический и мировоззренческий. Раньше эти приоритеты использовались весьма узкими, часто закрытыми, иногда тайными, иногда полумистическими элитарными сообществами, претендующими на управление мировыми процессами. Сегодня, в цифровом мире, они должны защитить массовое сознание от деградации и социальной деструкции.

Стремительно возрастающие потоки информации должны нести такие смыслы и направляться в такие русла, в которых они не будут дробить сознание народов, отуплять людей, порождать деструкцию, толкать на убийства и самоубийства.

Повышение эффективности противоборства разрушительным акциям информационной войны требует наполнения информационных сфер, социальных сетей, блогов, сайтов сети Интернет, средств массовой информации, культурно-образовательной среды мощным позитивным патриотическим контентом.

Такой контент должен быть сформирован на основе ясной идеологии, обосновывающей право на национальный суверенитет, на защиту традиционных духовных ценностей, на творчество в достижении высоких жизненных целей. Нужно целенаправленно создавать и мировоззренческий фон, который будет адекватен как научным представлениям о мироздании, так и духовным достижениям, раскрывающим глубокие смыслы существования человечества и цивилизационного развития. Наконец, требуется консолидированный подход к отечественной истории не как к «признанию российской катастрофы XX века», а как к героическому прошлому, наполненному великими свершениями и победами.

При последовательном использовании в информационном противоборстве высших приоритетов управления реактивная информация, давая идеологическую мотивацию и порождая энергию действий и поступков; ресурсная информация, связывая прошлое, настоящее и будущее и образуя мировоззренческую основу; фоновая информация, отражая окружающую реальность и наполняя смыслами общественные отношения и коммуникации, станут теми базовыми элементами, теми рычагами и инструментами, которые требуются для преодоления угроз социальной деструкции в условиях информационной войны против России.

Список литературы

1. Шмидт Э. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнесов и понятий государств / пер. с англ. – М. : Манн, Иванов и Фербер, 2013.

2. Уэбстер Ф. Теория информационного общества / пер. с англ. – М. : Аспект Пресс, 2004.

3. Овчинский А. С. Информационные воздействия и организационная преступность. – М. : Инфра-М, 2007.

4. Овчинский А. С. Информационные координаты: Управление. Противоборство. Безопасность / А. С. Овчинский, К. К. Борзунов, С. О. Чеботарева. – М. : Горячая линия. – Телеком, 2018. – 270 с.

5. Овчинский А. С. Матрица преступности / А. С. Овчинский, С. О. Чеботарева – М. : Норма, 2006.

6. Сундиев И. Ю. Теории и технологии социальной деструкции / И. Ю. Сундиев, А. А. Смирнов. – М. : Русский биографический институт; Институт экономических стратегий, 2016.

7. Фурсов А. И. Психоисторическая война: Скрытые субъекты глобального управления и фальсификация истории // Изборский клуб. – URL: Izbjrsk-club.ru/2439.

8. Ефимов В. А. Концептуальная власть. – М. : Издательский дом «Общественная инициатива», 2003.

Дуваа Антоний Анатольевич[1]**,**
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Поликарпов Евгений Сергеевич[2]**,**
доцент кафедры специальных информационных технологий УНК ИТ,
кандидат технических наук

СОВРЕМЕННЫЕ ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ ЗАРУБЕЖНЫХ СТРАН

Актуальная статистика свидетельствует о том, что число преступлений в сфере информационно-телекоммуникационных технологий только растет. По данным Генеральной прокуратуры Российской Федерации, в 2017 г. их количество увеличилось с 65 949 до 90 587. Доля таких преступлений от числа всех зарегистрированных в России преступных деяний составляет 4,4 %. Показатели первого полугодия 2018 г. также свидетельствуют о росте указанной категории преступлений (+3,4 %). Анализируя судебную и следственную практику, можно сделать вывод о том, что самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Количество мошенничеств с использованием платежных карт в 2018 г. выросло в 7 раз. Цифры неутешительные, тем более что раскрываемость преступлений в сфере информационно-телекоммуникационных технологий ежегодно колеблется в пределах 45–53 %.

В текущем году были зарегистрированы 180 153 киберпреступления. Это на 66,8 % больше показателя за аналогичный период предыдущего года, сообщает Генеральная прокуратура Российской Федерации на своем сайте. Речь идет о преступлениях, совершенных с использованием ИКТ или в сфере компьютерной информации. Генеральная прокуратура Российской Федерации характеризует рост киберпреступности как «весьма существенный». Если сравнивать с данными, которые ведомство приводит для других видов преступлений, темпы роста в этом сегменте оказываются самыми высокими.

В условиях постоянно меняющейся картины угроз важно понимать, в каком направлении развивается вектор кибератак и какие меры безопасности надо предпринимать. Западные страны сегодня выделяются наиболее развитой информационно-телекоммуникационной структурой и соответствующим уровнем киберпреступности, что большой долей вероятности отразится на отечественном сегменте информационно-телекоммуникационных сетей.

Вредоносное программное обеспечение, как и в прошлые годы, занимает лидирующие позиции. В 2018 г. были созданы 137,5 млн новых образцов вредоносного программного обеспечения (ПО), 93 % обнаруженных вредоносных

программ были полиморфными, что означает, что они могут постоянно изменять свой код, чтобы избежать обнаружения. Более 50 % устройств, которые были заражены один раз, были повторно заражены в течение того же года [1].

Национальное агентство по борьбе с преступностью в Великобритании сообщает, что киберпреступность в настоящее время составляет более 50 % всех преступлений.

Отчет об угрозах *ENISA* за 2018 г. показывает, что вымогатели по-прежнему являются серьезной причиной для беспокойства для любого типа организации в разных секторах, независимо от ее размера и сложности: 1) 39 % угроз нарушения целостности данных, вызванных вредоносным программным обеспечением, были совершены вымогателями; 2) 17 % от общего числа нарушений целостности данных здравоохранения Великобритании были связаны с вымогательством; 3) 66 % компаний признают, что вымогатели представляют серьезную угрозу, при этом менее 13 % из них были готовы к такой атаке в 2017 г.; 4) вымогатели наносят атаки на 15 % предприятий в 10 ведущих отраслях, таких как образование, IT и телекоммуникации, развлечения, финансовые услуги, строительство, правительство, производство, транспорт, здравоохранение и розничная торговля.

В наши дни к сети Интернет подключены больше незащищенных устройств, чем когда-либо, в связи с чем киберпреступники чаще наносят DDos-атаки и наносят более крупный ущерб нежели раньше. В месяц по всему миру регистрируются 400 тыс. DDos-атак [2].

С каждым годом злоумышленники становятся все хитрее при создании и отправке фишинговых писем, которым подвержены даже самые опытные пользователи. Мошенники рассылают около 6,4 млрд поддельных писем каждый день[3]. Отчет компании *Verizon* [4] сообщает, что 30 % фишинговых писем открываются в США, причем 12 % из тех, кто их открыл, переходят по зараженным ссылкам. Анализируя ежемесячно более 470 млрд сообщений, за 2018 г. количество фишинговых писем во всем мире увеличилось на 250 % [6]. В отчетах компании *Cofense Reporter* говорится, что 91 % кибератак осуществляется с помощью электронной почты, взлом которой начинался с фишинг-письма.

Спам все также считается одним из самых эффективных способов доставки вредоносного программного обеспечения. В отчете о состоянии киберпреступности *Secureworks 2018* привели статистику, в которой среднесуточный объем спама вырос до 295,62 млрд писем. 75 % спама чаще всего связано со здоровьем (26,6 %), доставкой вредоносного ПО (25,7 %), сайтами для онлайн-знакомств (21,4 %), остальные 25 % включают в себя поддельные предложения о работе, фишинговые письма, финансовые операции и др.

Количество пользователей во всем мире составляет примерно 5 млрд. В связи с этим киберпреступники имеют множество возможностей для реализации атак на платформе современных телефонов. Согласно исследованиям *ThreatMatrix* [5], мошенничество с использованием мобильных устройств в начале 2018 г. выросло на 24 % по сравнению с прошлым годом, также в первой половине года совершены более 150 млн атак. С 2015 г. размер мошенничества с помощью мобильных приложений увеличилось на 600 % [7]. Только в 2018 г. на американ-

ские телефоны было сделано более 26 млрд роботизированных звонков – на 46 % больше по сравнению с прошлым годом [8].

В сети хранится огромное количество личных и конфиденциальных данных, что является огромной проблемой нашего общества. Утечка данных – международная проблема, полностью защититься от которой не получается ни у одного государства. В организации *McAfee* [9] считают, что среднее количество записей, потерянных при взломе в 2017 г., составляло 780 тыс. в день. Чьи-либо личные данные легко можно купить в «темной сети», они в среднем могут стоить всего лишь 3 доллара США [10].

Киберпреступность представляет собой относительно новую криминальную сферу, но она уже сейчас приносит в год ущерб не менее 1,5 трлн долларов [11]. 15 млрд долларов – стоимость криптовалюты, украденной с онлайн-бирж в период с 2012–2017 гг. [12]. 13,5 млн долларов потерял индийский банк после того, как хакеры установили ВПО на сервер банкомата, что позволило им осуществлять снятие средств [13]. Средний ущерб для компании от одной атаки взлома данных составляет 3,8 млн долларов [14].

По оценкам аналитиков, к 2021 г. в мире не будет хватать 3,5 млн специалистов в области информационной безопасности [15]. В отчете по защите от киберугроз *Imperva 2019* 84 % организаций сталкиваются с проблемой нехватки навыков по защите информации. В 2018 году тремя наиболее востребованными должностями в США были: инженер по кибербезопасности, аналитик по кибербезопасности и сетевой инженер [16]. Среднегодовая зарплата инженера безопасности в США составляет 88 тыс. долларов, в Великобритании – 69 тыс. долларов. Аналитики же получают около 95 тыс. долларов.

Россия заняла 26-е место в рейтинге Глобального индекса кибербезопасности Международного союза электросвязи ООН (*Global Cybersecurity Index 2018*) с показателем 0,836 балла. В предыдущей редакции рейтинга, выпущенной в 2017 г., она занимала 10-е место с индексом 0,788 балла. Таким образом, Россия «просела» в списке на 16 позиций, однако сумела улучшить свой результат. Отметим, что в рейтинге 2014 г. она занимала 12-е место с индексом 0,5 балла.

Подводя итог вышесказанному, отметим, что борьба за безопасность киберпространства недостаточна на уровне отдельно взятых государств. Сама природа рассматриваемых преступлений, базирующаяся на открытом и общедоступном характере телекоммуникационных сетей и связанная с особенностями вопросов юрисдикции, а также специфики подхода правоохранительных органов к расследованию таких преступлений, способствует росту и развитию киберпреступности.

Для эффективной борьбы с глобальным явлением киберпреступности необходимо сотрудничество на международном уровне, на двусторонней и многосторонней основах посредством подписания договоров, соглашений и участия государств в международных организациях и конференциях. Необходима налаженная работа многостороннего механизма обмена информацией, своевременная система реагирования на киберпреступления и действующий механизм сотрудничества в области международной безопасности в киберпространстве. Для создания правовых основ борьбы с киберпреступностью необходимы базовые стандарты кибербезопасности и реагирования на глобальном уровне.

Список литературы

1. Отчет об угрозах Webroot за 2019 г.
2. URL: https://www.calyptix.com/top-threats/ddos-attacks-2018-new-records-and-trends/
3. URL: EY – Global information Security Survey, 2018–2019.
4. URL: https://enterprise.verizon.com/resources/reports/dbir/
5. URL: https://www.businesswire.com/news/home/20180912005231/en/Mobile-Fraud-Reaches-150-Million-Global-Attacks
6. Отчет Microsoft Security Intelligence
7. URL: https://community.rsa.com/docs/DOC-86796
8. URL: https://assets.hiya.com/public/pdf/RobocallRadar.pdf?v=df22cb9f7328cd8fa08540344c688902
9. URL: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html
10. URL: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf
11. Bromium In the Web of Profit - Понимание роста экономики киберпреступности
12. Отчет о глобальной безопасности Trustwave за 2018 г.
13. URL: https://www.infosecurity-magazine.com/news/indian-bank-loses-135m-in-global/
14. URL: https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/advanced-threat-analytics
15. URL: https://cybersecurityventures.com/jobs/
16. URL: https://www.cyberseek.org/heatmap.html

Кирюхин Артем Викторович[1]**,**
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Поликарпов Евгений Сергеевич[2]**,**
доцент кафедры специальных информационных технологий УНК ИТ,
кандидат технических наук

ОБЗОР СОВРЕМЕННЫХ ИНСТРУМЕНТОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Современные технические средства защиты информации достигли уровня, когда на взлом затрачивается много времени либо цена защищаемой информации намного меньше расходов на ее добывание. Поскольку в любой организации работают люди, неизбежно возникает влияние человеческого фактора на все ее процессы. К сожалению, непредсказуемость поведения человека может уничтожить даже самые безопасные информационные системы.

Обратимся к статистике. Самым распространенным видом кибермошенничества – более 80% случаев – в 2018 г. стала социальная инженерия, в 11 % – вредоносное программное обеспечение, в 8 % – другое и в 1 % – скимминг [2]. Согласно статистике, чаще всего атаки социальной инженерии осуществляются с помощью звонков.

Социальную инженерия можно классифицировать по типу атаки:

- претекстинг;
- фишинг;
- обратная СИ;
- фарминг;
- троянский конь;
- *dumpster diving*;
- *waterholing*;
- приманка;
- «кви-про-кво» (лат. *qui pro quo* – вместо другого);
- плечевой серфинг;
- *tailgating*.

По используемому каналу:

- *e-mail*;
- *IM*;
- телефон;
- социальные сети;
- облачные сервисы;
- веб-сайты.

Перейдем к обзору инструментов социальной инженерии. Обратимся к операционной системе *Kali Linux*. В ней имеется предустановленная утилита *Social-Engineer Toolkit* (*SET*), предназначенная для социальной инженерии. Данная утилита имеет множество возможностей. Продемонстрируем одну из них – создание фишингового сайта.

Вызовем утилиту, используя команду *setoolkit*.

В окне терминала появится приветственное окно, в котором предлагается выбрать интересующий нас пункт. Мы хотим получить учетные данные жертвы от социальной сети «ВКонтакте», поэтому нужно сделать клон оригинальной страницы. Выбираем *Social-Engineering Attacks – Website Attack Vectors – Credential Harvester Attack Method – Site Cloner*. Появится сообщение: «*Tabnabbing: Your IP Address*», в котором необходимо ввести свой IP-адрес. Следующий шаг – создание клона сайта. Для этого необходимо ввести *URL* веб-страницы, копию которой хотим создать, в формате: *http://www.originalsait.com* (*рис. 1*). Далее утилита сообщает о том, что ведется создание и настройка веб-сайта.

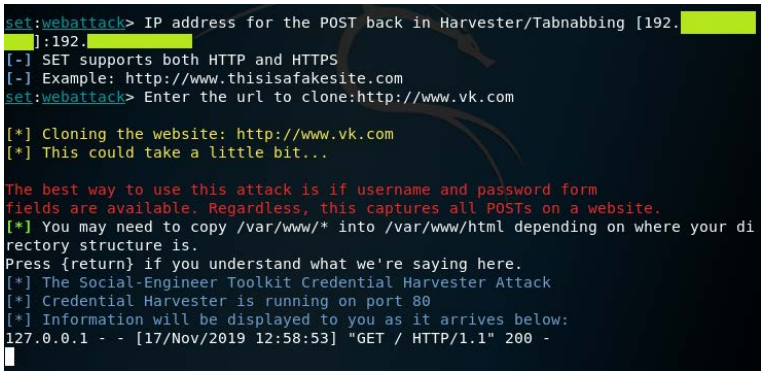

Рис. 1. Создание фишингового сайта

Чтобы перейти по ссылке, созданной *SET*, необходимо перейти по ссылке: (http://IP-адрес, введенный при создании клона). Ссылку можно сократить с помощью таких служб, как *ADF.LY, Binbox, Goo.gl* и т. д. или сгенерировать QR-код, содержащий данную ссылку. Как только мы введете свой IP-адрес на этих сайтах для сокращения, они предоставят короткую ссылку, и все, что вам нужно сделать, это просто отправить эту сокращенную ссылку или QR-код своей жертве. Когда жертва посетит URL-адрес, который был ей отправлен, она увидит ту же страницу, *URL* которой вводился для клонирования.

Жертва будет думать, что это оригинальная страница, и когда жертва введет свои учетные данные, они будут отображаться в окне терминала (эти данные можно посмотреть в */var/www/harvester*). Также в окне терминала отображаются дата и время обращения к созданному фишинговому сайту и IP-адрес, с которого зафиксировано обращение (*рис. 2*).

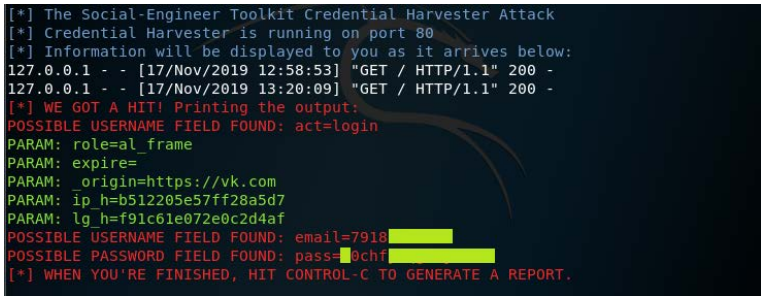

Рис. 2. Учетные данные жертвы

Также в *Kali Linux* имеется встроенный инструмент для генерации *QR*, которой входит в *SET*. Заходим в пункт *Social-Engineering Attacks*, затем выбираем *QRCode Generator Attack Vector*. Вводим текст, который хотим поместить в QR-код или *URL* веб-сайта. Сгенерированный QR-код по умолчанию сохраняется в */root/.set/reports*.

Рассмотрим инструмент *TrackUrl* для операционной системы *Kali Linux*, который позволяет узнать местоположение человека, используемую операционную систему, версию браузера. В скрипте инструмента используются *HTML5* и *JavaScript*. Для того, чтобы использовать *TrackURL* вне локальной сети, используется *Ngrok* – платформа, которая с помощью установленной утилиты позволяет организовать удаленный доступ на веб-сервер или какой-то другой сервис, запущенный персональным компьютером (ПК). Доступ организуется через созданный при запуске *ngrok* безопасный туннель, ПК при этом может находиться за *NAT*[1] и не иметь статического IP-адреса.

Для начала необходимо скопировать репозиторий с *GitHub* командой:

git clone https://github.com/Mauladen/TrackUrl.git

Затем переходим в папку, и проверяем наличие файлов:

cd TrackUrl/ls.

Для корректной работы *TrackUrl* нам нужно изменить разрешения некоторых файлов, а именно: *TrackUrl.sh* и *ngrok*. Затем запускаем скрипт:

./TrackUrl.sh.

В результате данной операции должны открыться два окна терминала:

В поле *URL* окна *TrackUrl* необходимо ввести ссылку, которая указана в *Forwarding*, именно благодаря ей мы сможем обойти *NAT*.

При желании ссылку можно сократить через специальные сервисы или сгенерировать QR-код, в котором будет содержаться ссылка на наш сайт.

Как только жертва перешла на сайт, в нашем терминале показываются дата перехода, браузер жертвы, используемая операционная система и ее разрядность, местоположение жертвы. Когда жертва разрешит доступ к данным своего местоположения, мы получим об этом оповещение в окне терминала *ngrok* (*рис. 3*).

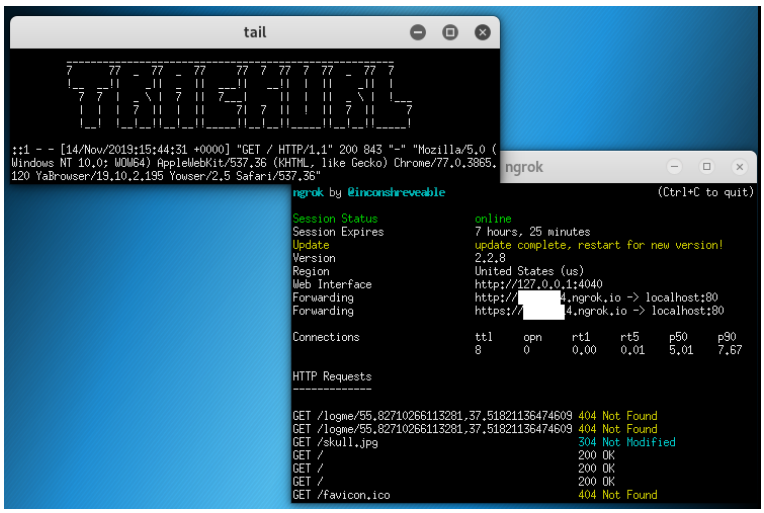

Рис. 3. Полученные данные

Осталось ввести полученные координаты в сервисах (онлайн-картах), после чего мы увидим местоположение человека. Данный инструмент может использоваться при многих атаках социальной инженерии, например, при фишинге.

[1] *NAT* – (англ. *Network Address Translation* – «преобразование сетевых адресов») – это механизм в сетях *TCP/IP*, позволяющий преобразовывать IP-адреса транзитных пакетов (NAT // URL: https://ru.wikipedia.org/wiki/NAT).

Обратимся к другому инструменту для *Kali Linux – Pentbox*, с помощью которого можно создать *Honeypot* (англ. – «горшочек с медом») является своего рода ловушкой для хакера, но его можно использовать и в социальной инженерии с целью получения информации о пользователе. Для начала необходимо скачать и распаковать утилиту при помощи команд:

wget http:/downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz

tar-zxvf pentbox-1.8.tar.gz

Теперь необходимо перейти в директорию, где установлена утилита с помощью команды:

cd pentbox-1.8/

Запустим Pentbox, используя команду:

./pentbox.rb

Перед нами появилось приветственное окно утилиты, где необходимо выбрать интересующий пункт. Поскольку мы хотим создать *Honeypot*, то переходим во вкладку *Network Tools*, а затем выбираем *Honeypot*.

Затем утилитой будет предложена настройка *Honeypot*. Можно выбрать автоматическую настройку или настроить вручную. При выборе автоматической настройки для *Honeypot* будет назначен 80-й порт, а при переходе по ссылке будет отображаться стандартный текст. Если выбрать ручную настройку, то можно назначить *Honeypot* конкретный порт и ввести любое сообщение, которое будет отображаться при посещении ссылки.

«Горшочек с медом» готов, теперь необходимо перейти на страницу *http://192.168…*, на который запущен *Honeypot*.

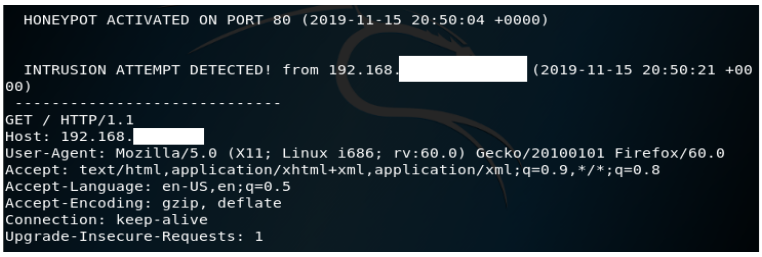

Рис. 4. Информация об устройстве жертвы

В терминале появится сообщение «HONEYPOT ACTIVATED ON PORT 80» и «INTRUSION ATTEMPT DETECTED», и будет представлена информация об устройстве, с которого был осуществлен переход по ссылке (*рис. 4*).

Список литературы

1. Поликарпов Е. С. Компьютерная разведка : учебное пособие / Краснодарский университет, 2018.
2. «Threat Zone ‘19: Иллюзия безопасности» Bi Zone, М., 2019.
3. «THREAT ZONE 17/18» Bi Zone. M., 2019.
4. Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl Advanced Social Engineering Attacks. SBA Research, Favoritenstrae 16, AT-1040 Vienna, Austria. – 2014.
5. URL: https://www.knowbe4.com/what-is-social-engineering.
6. URL: https://www.social-engineer.org/framework/attack-vectors/attack-cycle.

7. URL: https://habr.com/ru/post/83415.
8. URL: https://github.com.
9. URL: https://ru.wikipedia.org/wiki/NAT.
10. URL: https://xaker.ru.

Пытайло Алексей Владимирович[1],
начальник департамента производства и эксплуатации ООО «БалтИнфоКом»

ИНТЕГРАЦИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ КАК СЕГМЕНТА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационно-аналитическая работа сегодня включает в себя работу с большими массивами данных, с сервисами и сегментами глобальной сети, а также при взаимодействии частных и государственных компаний и организаций, а именно: биллинг сетей сотовой, спутниковой и иной связи; данные с камер видеонаблюдения; личные или сторонние базы данных; данные с систем контроля доступа; данные с радиозакладных устройств или трекинговых систем; данные о покупке и использовании билетов; данные о банковских транзакциях; данные, взятые из открытых источников (социальные сети, новостные ресурсы, доски объявлений и т. д.); данные текстового формата (документы, договоры, рапорты, статьи резюме и т. д.).

Результат аналитической деятельности. Результат аналитической работы – это чаще всего список идентификаторов. Изначальный массив идентификаторов огромен при практически любой задаче. Изначальный массив можно фильтровать по различным критериям, в том числе по ГЕО, по связям, по классификаторам и др. Один из основных и универсальных способов фильтрации – это пересечение списков, т. е. уменьшение размера списка за счет другого списка. Создание списка на основании зонта требует указание зонта, типа списка и «нахождения в зонте». В том случае, если списку не будет присвоено имя, он будет временным и будет удален при перезагрузке ПО. Тип списка «Выбор типа входящих в список из зонта данных»: сток-список; список телефонных номеров (*MSISDN*); список терминальных номеров (*IMEI*); список системных номеров (*IMSI*); список временных номеров (*TMSI*); список тюплов; список абонент-векторов.

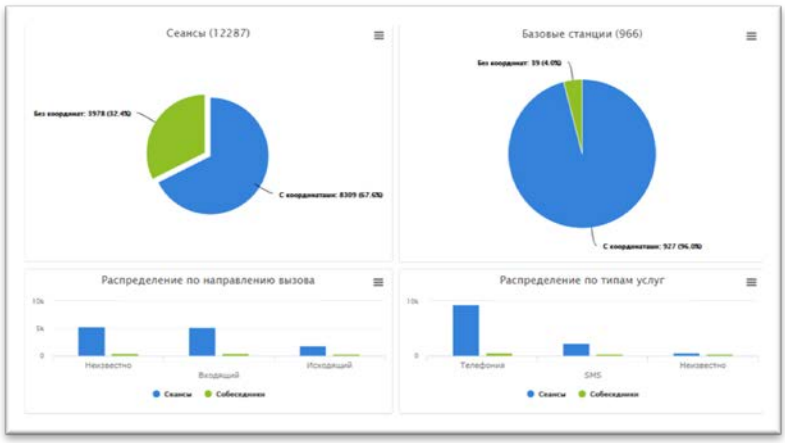

Рис. 1. Анализ активности объекта исследования – связь

Спектр задач, выполняемый аппаратно-программными комплексами и решениями: выполнение заданий по поиску информации в сети Интернет; предоставление пользовательского интерфейса по «ручному» формированию заданий на поиск информации в сети Интернет; фоновая выгрузка «случайной» информации из сети Интернет; предоставление средств мониторинга статуса выполнения заданий; мониторинг социальных сетей; поиск по ключевым словам и принадлежности к сообществам социальных сетей; сбор информации в онлайн-базах данных; мониторинг результатов выполнения запросов к поисковым системам; мониторинг сайтов объявлений; мониторинг новостных сайтов, поддерживающих формат *RSS*, и извлечение новостной информации; мониторинг коммерческих справочных интернет-систем морского транспорта; отслеживание изменений собранной информации с заданной периодичностью, – все это позволяет быстро и эффективно производить сбор, анализ и визуализацию материалов по исследуемому лицу.

Сбор метеорологических данных из открытых источников; выгрузка по запросу информации из реестра запрещенных ресурсов сети Интернет Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций; управление заданиями для поиска и загрузки информации из указанных источников предоставляет актуальные данные в режиме реального времени, что позволяет сократить время на формирование запросов в государственные и иные структуры по вопросам предоставления оперативно значимой информации.

Рис. 2. Список идентификаторов

В целом, подготовка специалистов в области информационной безопасности определена в документах стратегического планирования как одно из наиболее важных и приоритетных направлений в современном мире, в особенности – при формировании аппарата кадров подразделений правоохранительных органов. Функционирование подразделений правоохранительных служб, сопряженных с получением, обработкой и анализом информации, поступающей из различных источников, связано с систематическим совершенствованием инструментария, обеспечивающего эффективность выполнения задач специального типа и, в частности, при формировании итоговой документации в виде аналитических материалов на лицо или группу.

Рахимова Ирина Олеговна[1]**,**
курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я, Кикотя

Гончар Владимир Владимирович[2]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Информационное общество – это новейшая сфера развития современного человека, на которой главными атрибутами производства становятся информационные знания. Переход к информационному обществу часто называют информатизацией. Об этом можно судить по следующим признакам: использование различных информационных технологий во всех сферах жизнедеятельности общества и государства в целом; развитие средств связи (коммуникаций); обучение компьютерной грамотности любого человека; свобода доступа к любой информации; развитие дистанционного образования с использованием сети Интернет; изменение экономической структуры с точки зрения информатизации.

В результате индустриализации машины заменили человека, а в результате информатизации компьютеры начинают самостоятельно собирать и обрабатывать информацию, заменяя умственный труд человечества. Одним из признаков исследуемого общества можно выделить – обширное введение цифровизации во все сферы жизни общества и государства в целом.

Культура общества в компьютерной сфере – это деятельность общества, направленная на использование различных информационных ресурсов, а также средств и методов по обмену информацией; использовать достижения и передовые информационные технологии. Информатизация общества целиком зависит от компьютеризации и внедрении новых способов взаимодействия. Информационное общество – общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей ее формы – знаний [5, с. 32]. Если углубляться в изучение развития компьютерной техники и информационных технологий, то они дают обширные возможности для дальнейшего развития общества. Новации в сфере компьютеризации – это различные программы, включающие различную компьютерную технику для хранения, защиты, обработки и передачи информации.

К информационным технологиям относятся: разработка различного типа документов; поиск информации; использование компьютерной сети (сеть Интернет, электронная почта); автоматизация систем управления (создание и применение

АСУ); САПР (внедрение систем автоматизированного проектирования); геоинформационные системы (внедрение систем на основе карт и снимков со спутника).

Государственные информационные системы (ГИС) создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях [1].

Географическая информационная система предназначена для сбора, хранения, анализа, графической визуализации пространственных данных.

Говоря языком географии, ГИС – это инструменты, которые дают возможность искать, анализировать, редактировать цифровые карты и необходимую дополнительную информацию о каких-либо объектах.

ГИС широко применяются в картографии, геологии, метеорологии, землеустройстве, экологии, муниципальном управлении, транспорте, экономике и обороне.

По объему территории ГИС могут быть: глобальные; субконтинентальные; национальные; региональные; субрегиональные; локальные или местные. Пространственными данными являются такие, которые описывают местоположение объектов в пространстве, а ГИС дают возможность добавлять, удалять, обновлять, запрашивать, просматривать, анализировать эти данные. Пространственные данные представлены в виде основных форматов – векторной графики и в виде растров.

Растровое изображение – это двумерный массив точек, где каждая точка представлена своим цветом. Для оформления «подложки» цифровой карты обычно используется растровая графика, а поверх ее отображается векторная геометрия. Например, на картах Яндекс можно увидеть огромное количество растров.

Пространственной информацией можно отображать огромное количество при небольших объемах памяти, и это, без сомнения, большой плюс растровых изображений на цифровых картах.

Отрицательным моментом, пожалуй, является то, что при увеличении масштаба отображения, качество изображения на растре значительно снижается. Вполне понятно, что разные масштабы будут использовать растры разного территориального охвата и разрешения. Они будут сменять друг друга, если картинку надо будет увеличить или уменьшить.

Векторная графика. Это не что иное, как геометрия, представленная в виде наборов координат. Само изображение не хранится, под системой визуализации оно формируется «налету» и, независимо от масштаба, имеет высокое качество картинки.

Виды векторных пространственных данных:

1) точечная геометрия. Чаще всего, это точка на карте определенного цвета. В ряде случаев ГИС заменяют эту точку стрелкой, иконкой, растровым рисунком, векторным символом;

2) линейная геометрия. Использование этого вида целесообразно тогда, когда важно показать протяженность и площадь. Такими объектами, как правило, являются дороги, реки, территориальные границы и др.;

3) площадная геометрия. Использовать этот вид будут тогда, когда важным является абсолютно все [6, с. 102].

Карты удобно использовать как базовый слой ГИС. При отсутствии информации о данной изучаемой территории цифровизируются оригиналы карт. К ним относятся данные, полученные с космических носителей. При их использовании применяются разные технологии для получения изображений и передачи их на Землю, носители аппаратуры для съемки (космические аппараты и спутники) размещаются на разных орбитах, оснащаются различной аппаратурой.

Таким образом, получаются снимки, которые отличаются различным уровнем обзора и детализации отображения объекта природной среды в различных диапазонах спектра (видимом и ближнем инфракрасном, тепловом инфракрасном и радиодиапазоне). Это способствует решению широкого спектра экологических задач с использованием ДДЗ. На основе ГИС возможно при расследовании преступлений использовать технологию ситуационного моделирования с использованием геоинформационных систем.

Развитие информационных технологий в указанной сфере способствовало появлению автоматизированных информационных систем (АИС). Их применение реализуется для разыскных мероприятий (ГИС «Зеркало», АГИПС «Сова»). Данное программное обеспечение, являющееся средством информационных технологий, помогает сотрудникам разного уровня в расследовании преступлений [7].

Исследуя теорию и практику оперативно-разыскной деятельности (ОРД), а также новации в области ИКТ, основанные на средствах различной цифровизированной техники и методах в области математики, можно утверждать, что это способствует формированию такого направления в деятельности органов внутренних дел, как аналитическая работа в сфере ОРД, и одной из ее форм оперативно-разыскного прогнозирования (ОРП), которые принято рассматривать на двух уровнях: стратегическом и тактическом [8].

В качестве функций оперативно-тактического прогнозирования принято выделять прогнозирование:

– возможной тактики преступных группировок и нелегализированных объединений с девиантной направленностью – для определения необходимости, форм и методов профилактического вмешательства;

– возможной обстановки, которая может возникнуть в период их оперативной проверки;

– вероятного поведения лиц, оказывающих содействие органам, уполномоченным на осуществление оперативно-разыскной деятельности в определенных условиях [9].

На данный день на практике выделяется и разрабатывается несколько программных материалов, которые позволяют воспроизводить прогноз различных значимых объектов для оперативных подразделений благодаря методам компьютерной обработки информации.

Например, на базе отделения оперативно-разыскного прогнозирования Центра оперативно-разыскной информации ГИАЦ МВД России (далее – подразде-

ления ОРИ) была разработана и стала применяться специализированная геоинформационная система – ГИС «Зеркало» [10].

Анализируя вышеизложенный материал, мы можем сделать ряд выводов относительно новаций развития различных способов применения информационных технологий и цифровых программ на практике для осуществления оперативно-разыскного прогнозирования:

1. В будущем развитие разыскного прогноза в целях поиска данных будет обосновано необходимостью цифровизации всей совокупности прогностических подсчетов.

2. Вспомогательные компьютерные технологии следует признать необходимым методом анализа при раскрытии преступлений, который помогает осуществлять аналитические исследования в оперативных подразделениях с использованием инновационных методов.

3. Усовершенствование новейших компьютерных технологий и атрибутов позволит повысить уровень и объем оперативно-разыскного прогноза.

4. Появление цифровых программ прогнозирования в оперативных подразделениях должно быть вспомогательной составляющей при выработке соответствующих способов прогноза оперативно значимых объектов.

5. Необходимой средой появления значимых результатов прогноза с помощью вспомогательных компьютерных технологий является совокупное использование аналитических методов, таких как: математических и экспертных оценок.

6. Во время использовании сложнейших компьютерных технологий для прогноза в оперативных подразделениях логично организовать проведение специальных подготовительных курсов на базе учебных (научных) заведений [11].

Следовательно, опыт цифровизации компьютерных программ во время расследования следует признавать важнейшим и успешным, так как это уже позволило существенно оптимизировать принятие управленческих и оперативно-тактических решений в ходе осуществления оперативно-разыскной деятельности [12].

Список литературы

1. Федеральный закон от 27 июня 2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» // Собр. законодательства Рос. Федерации. – 2006. – № 31 (1 ч.). – Ст. 3448.

2. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 (ред. от 11.04.2019) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации» // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 08.07.2015).

3. Агеев В. В. Об опыте компьютеризации оперативно-розыскного прогнозирования // Информационное право. – 2011. – № 1. – С. 19–23.

4. Алымов Д. В. Основные направления развития научно-технического обеспечения правоохранительной деятельности // Известия Юго-Западного гос-

ударственного университета. – Серия: История и право. – 2018. – Т. 8. – № 2 (27). – С. 8–91.

5. Амелин Р. В. Правовой режим государственных информационных систем : монография / под ред. С. Е. Чаннова. – М. : ГроссМедиа, 2016. – 338 с.

6. Амелин Р. В. Правовые отношения в сфере создания и использования государственных информационных систем // Административное и муниципальное право. – 2017. – № 9. – С. 32–49.

7. Аминев Ф. Г. Актуальные проблемы ситуационного моделирования в судебно-экспертной деятельности // Эксперт-криминалист. – 2013. – № 3. С. 12–14.

8. Белоглазов Е. Г. Методология обеспечения аналитической разведки процессов и явлений : автореферат диссертации … д-ра юрид. наук. – М., 2007. – 45 с.

9. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

10. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельности: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

11. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

12. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Рудакова Наталия Константиновна[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Поликарпов Евгений Сергеевич[2]***,***
доцент кафедры специальных информационных технологий УНК ИТ,
кандидат технических наук

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ СИСТЕМ ФИЛЬТРАЦИИ КОНТЕНТА В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ РОССИЙСКОЙ ФЕДЕРАЦИИ

Развитие компьютерных технологий и электронных средств массовой информации привело к формированию единого мирового информационного пространства, которое открывает множество новых возможностей. В настоящее время, как всем известно, сеть Интернет наполнена не только полезными ресурсами, но и нежелательным контентом.

На данный момент существует проблема ограничения доступа обучающихся к различного вида информации посредством сети Интернет в образовательных организациях. Результаты проверок, ежегодно осуществляемых в учебных заведениях, нередко показывают нарушения в области обеспечения защищенного доступа обучающихся к различного рода информации с технического оборудования, установленного на территории образовательных организаций.

Решить данную проблему представляется возможным с помощью прокси-сервера либо контент-фильтра.

Реализовав использование прокси-сервера, образовательное учреждение будет обладать возможностью управления доступом в сеть Интернет со всех технических средств, установленных на его территории. Также появится возможность включения и отключения прокси-сервера в то время, когда это будет необходимо. Еще одним главным преимуществом является предоставление полного контроля образовательной организации за использованием сети учащимися, т. е. можно будет полностью просматривать временной промежуток и статистику посещения ими различных сайтов. Дополнительно существует еще одно преимущество, которое заключается в том, что при желании можно запретить скачивание определенных типов файлов.

С 2006 г. федеральные органы государственной власти Российской Федерации занимаются проведением большого количества различных мероприятий, которые направлены на обеспечение ограничения доступа обучающихся к деструктивной информации посредством сети Интернет в образовательных учреждениях. Выполнить эту задачу предлагается с помощью систем фильтрации контента – так называемых контентных фильтров.

Под контентным фильтром мы понимаем такое специальное программное обеспечение, которое предназначено для фильтрации интернет-сайтов, содержащих негативную информацию для просмотра.

Принцип работы контентного фильтра заключается в проверке адреса запрашиваемого сайта с помощью черных списков адресов. Данные списки необходимо постоянно обновлять, так как ежедневно появляется большое количество новых источников информации подобного деструктивного характера, но в силу изменения наименования адресов все они уже являются потенциально новым контентом.

Существует несколько способов реализации фильтрации контента:

1. Фильтрация на государственном уровне: централизованный подход к фильтрации контента государством.
2. Фильтрация на уровне поставщика: осуществляется провайдерами путем создания списков запрещенных ресурсов, ориентирующегося на государственные источники такой информации, а также на судебные решения.
3. Фильтрация на уровне интернет-шлюза: предполагается настроить сетевой шлюз, через который проходит интернет-трафик всех компьютеров или других устройств в сети.
4. Фильтрация на уровне рабочей станции: требуется установка специального (программного обеспечения) ПО непосредственно на сами компьютеры пользователей.

Фильтрация контента в образовательных учреждениях является обязательным требованием законодательства.

Так, в ст. 14 Федерального закона от 28 декабря 2017 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» закреплено требование об организации доступа к сети Интернет при условии применения административно-организационных мер, технических, программно-технических средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Существуют также Методические рекомендации по ограничению доступа обучающихся в образовательных учреждениях к видам информации, распространяемой через сеть Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей целям образования.

Следующим является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». В нем содержится определенный алгоритм логического ограничения доступа к информации, запрещенной к распространению на территории Российской Федерации в сети Интернет.

Основным с нашей точки зрения является Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации». В соответствии с ч. 2 п. 6 ст. 28 и чч. 8–9 п. 1 ст. 41 в обязанности образовательной организации входят вопросы, связанные с безопасностью и охраной здоровья обучающихся на территории образовательной организации.

Таким образом, образовательные организации в рамках своей работы должны обеспечивать информационную безопасность своих подопечных.

Рассмотрев все вышеперечисленные документы, мы можем убедиться в том, что системы контентной фильтрации очень необходимы и являются эффективным средством решения задач информационной безопасности обучающихся.

Разработкой контентных фильтров занимаются многие компании, среди которых довольно популярны следующие системы:

- личный фильтр контента *Net Police*;
- фильтр содержимого *SkyDNS*;
- автоинспектор.

Рассмотрим еще несколько примеров ПО в области фильтрации контента:

1. *UserGate Proxy & Firewall*.
2. *KinderGate*.
3. *SkyDNS*.
4. Интернет Контроль Сервер.
5. Интернет-цензор.

Вышеперечисленные программные продукты также включены в Единый реестр российских программ для электронных вычислительных машин и баз данных, а следовательно, утверждены государством.

Подводя итоги и сравнивая два представленных выше способа решения проблем ограничения доступа обучающихся к интернет-ресурсам в образовательных учреждениях, можно сделать вывод о том, что на данный момент практическая база применения контент-фильтров все же шире, чем у прокси-серверов, хотя у каждого из которых существует большой ряд преимуществ в применении.

Если обратить внимание на современные условия обучения подростков, то можно отметить тот факт, что не все общеобразовательные учреждения стараются организовать безопасность доступа обучающихся к разному роду контента. Даже если и существуют попытки данного процесса, то они, к сожалению, не в полной мере реализуются на всем техническом оборудовании.

С нашей точки зрения, данная тема актуальна и требует дальнейшего детального многостороннего изучения, поскольку установка и правильная настройка контентных фильтров в образовательных учреждениях позволяют эффективно защитить обучающихся от посещения и просмотра нежелательного контента, который может либо навредить обучающемуся, либо не относиться к сфере образования и тем самым способен снизить его уровень знаний, умений и навыков, являющихся основой для всего дальнейшего жизненного пути.

Список литературы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
2. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
3. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».
4. Федеральный закон от 28 декабря 2017 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Сергеева Елена Евгеньевна[1]*,*
курсант факультета подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]*,*
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ПРЕДВАРИТЕЛЬНОЕ РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 159.6 УК РФ

Актуальность данной темы обусловлена тем, что компьютерные преступления в наше время стали очень распространенными. С недавнего времени через сеть Интернет стало совершаться большое количество преступлений различной степени тяжести и различного характера. Но в российском законодательстве не было конкретных норм, которые предусматривали ответственность за совершение компьютерных преступлений. Данная проблема породила принятие Федерального закона от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», который ввел в Уголовный кодекс ряд экономических преступлений, предусматривающих ответственность за совершение квалифицированных видов мошенничества, в том числе и ст. 159.6 УК РФ, имеющую схожий состав с общественно опасным деянием, предусмотренным ст. 159 УК РФ «Мошенничество», но представляющий меньшую общественную опасность, что влечет менее строгий вид наказания, а также существенно изменил механизм правового регулирования уголовного преследования преступлений [1].

Включение указанных статей, содержащих в себе преступления в экономической сфере, способствует конкретизации компьютерных преступлений, однако это порождает ряд проблем [2].

Для рассмотрения вопросов, связанных с осуществлением предварительного расследования по уголовным делам о мошенничестве в сфере компьютерной информации, необходимо рассмотреть характеристику данного общественно опасного деяния.

Статья 159.6 УК РФ включает в себя четыре части, первая из которых раскрывает понятие мошенничества в сфере компьютерной информации, а вторая – четвертая части указанной статьи содержат квалифицированные составы данного преступления по признакам:

1) деяния, совершенного группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, предусмотренного ч. 2 ст. 159.6 УК РФ;

2) совершения лицом уголовно наказуемого деяния с использованием своего служебного положения; в крупном размере; с банковского счета, а равно

в отношении электронных денежных средств, предусмотренного ч. 3 ст. 159.6 УК РФ;

3) совершения организованной группой либо в особо крупном размере деяния, предусмотренного чч. 1–3 настоящей статьи и закрепленного в ч. 4 ст. 159.6 УК РФ[1].

Анализ состава данного преступления позволяет сделать вывод, что общественными отношениями, охраняемыми уголовным законодательством, при мошенничестве в сфере компьютерной информации одновременно выступают два объекта, а именно: компьютерная информация и имущество, что является одним из основных разграничений деяний, предусмотренных ст. 159.6 УК РФ, и при иных форм мошенничества[2].

Объективную сторону составляет хищение чужого имущества или приобретение права на чужое имущество.

Способами совершения преступления выступают: ввод, удаление, блокирование, модификация компьютерной информации и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [3].

Рассматривая субъективные признаки преступления, необходимо сказать, что по смыслу ст. 159.6 УК РФ субъектом является физическое вменяемое лицо, достигшее на момент совершения деяния 16-летнего возраста (общий субъект).

Субъективная сторона преступления выражена умышленной формой вины в виде прямого умысла.

Органы предварительного расследования на различных стадиях уголовного процесса сталкиваются с большими трудностями при раскрытии, расследовании и предупреждении мошенничества, совершаемого в сфере компьютерной информации. Расследование связано с определенными специальными знаниями, в связи с чем затрудняется обычный порядок предварительного расследования преступлений [4].

Согласно статистике Агентства правовой информации за 2018 г., по ст.ст. 159 и 159.1–159.6 УК РФ была рассмотрена 31 474 дел, по которым осуждены 24 195 лиц, 54 из которых – по ст. 159.6, что позволяет сделать вывод о том, что данные преступления являются наиболее сложно раскрываемыми для сотрудников органов внутренних дел, а в первую очередь – для лиц, осуществляющих предварительное расследование[3].

Точность и полнота расследования преступного деяния зависят от правильности выбранного направления следственной работы, которое было составлено при предварительной проверке информации по рассматриваемому делу лицом, осуществляющим предварительное расследование, тщательном анализе и оцен-

---

[1] «Уголовный кодекс Российской Федерации» от 13 июня 1996 г. №63-ФЗ (ред. от 04.11.2019).

[2] Уголовное право Российской Федерации: Общая часть. / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева / 2-е изд. – М. : Контракт; Инфра-М, 2008.

[3] Статистика Агентства правовой информации за 2018 г. по ст.ст. 159 и 159.1–159.6 УК РФ [Электронный ресурс] // URL: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/11/s/1.

ке существующей информации, выдвижении версий о подлежащих установлению обстоятельствах преступления.

При анализе элементов плана расследования мошенничества в сфере компьютерной информации в первую очередь необходимо установить первоначальные следственные действия для противодействия утраты источников доказательственной информации, интенсивность поиска, обнаружения, закрепления доказательств о событии преступления, изучение его обстоятельств и лиц, совершивших преступное деяние, выявления обстоятельств, способствовавших совершению преступления, розыск и задержание подозреваемых. В связи с этим действиям характерны максимальная оперативность и неотложность.

Ученые выделяют три типичные ситуации условий, в которых преступник совершил деяние, предусмотренное рассматриваемой нами статьей, закрепленной в УК РФ.

1. Преступление совершено при известных обстоятельствах, потерпевший выявил преступника самостоятельно, вследствие чего он был задержан, т. е. в условиях очевидности.

2. Правоохранительным органам известен способ совершения преступления лицом, который скрылся от должностных лиц, но полный механизм совершения преступления неясен.

3. Лицам, осуществляющим предварительное расследования, неизвестен ни механизм преступления, ни лицо, его совершившее. Налицо имеется только преступный результат.

В каждой из рассматриваемых ситуаций возникают сложности у правоприменителя в грамотной, полной и точной квалификации рассматриваемой разновидности мошенничества, также степень профессиональной квалификации субъектов расследования не всегда в полной мере соответствует современным требованиям, что, безусловно, не может не сказаться на качестве предварительного расследования по квалифицированному виду мошенничества.

Среди наиболее часто проводимых следственных действий правоохранительными органами являются:

1. Проведение осмотра места происшествия, а также предметов и документов. Основной проблемой при производстве данного следственного действия является трудность обнаружения места совершения преступления, т. е. у правоохранительных органов возникает ситуация производства обыска компьютера подозреваемого, а искомая информация находится на запоминающем устройстве, имеющем другое нахождение или доступном исключительно в виртуальной сети.

2. Допрос лиц с определенным процессуальным статусом. В круг данных лиц входят подозреваемые и обвиняемые, а также свидетели и потерпевшие. Необходимо отметить, что при выборе тактики и методики проведения допроса, определения отдельных тактических приемов правоохранительные органы руководствуются объемом информации о совершенном преступлении. Так как у лиц, проводящих допрос, в основном отсутствуют специальные знания в данной области, возникает необходимость в привлечении специалиста для проведения допроса. Но при этом необходимо учесть, что с противоположной

стороны данного следственного действия может возникнуть сопротивление, вызванное привлечением дополнительных лиц. Один из участников, который входит в перечень лиц, вызванных на допрос, начинает осознавать, что у лица, проводящего допрос, отсутствует необходимый круг знаний о технических особенностях, которые были применены преступником, способах, особенностях совершения преступления. Все сомнения допрашиваемого приводят его к выводу некомпетентности следователя в данном вопросе.

Наличие у допрашиваемых лиц желания оказать содействие расследованию может перечеркнуться отсутствием знаний у лица, осуществляющего расследование, что формирует отрицательное отношение к нему как к профессионалу своего дела.

Все это способствует представлению общей картины неспособности правоохранительных органов объективно расследовать исследуемые случаи мошенничества в сфере компьютерной информации, что особенно характерно для таких участников судопроизводства, как потерпевшие. Укрепившись в своей позиции о том, что у следователя отсутствуют необходимые знания в той сфере, в которой он производит расследование, потерпевший настраивается на то, что преступление не будет раскрыто, виновный не понесет наказания, а ущерб ему не будет возмещен, в силу чего у него полностью пропадает желание сотрудничать с правоохранительными органами.

3. Назначение и производство судебных экспертиз. В большинстве случаев эффективность судебных экспертиз в процессе расследования преступлений низкая, так как нет перечня вопросов, которые выносятся на разрешение эксперта и на которые в результате можно получить ответы, что делает судебные экспертизы неэффективными в производстве предварительного расследования. Данная проблема порождает необходимость разработки основных методик по назначению экспертиз.

4. Обыск и выемка.

5. Контроль и прослушивание телефонных и иных переговоров. Следует отметить, что использование данного следственного действия осложнено тем, что из буквального смысла закона не ясно, кому может быть поручено техническое осуществление контроля и записи переговоров: оперативному подразделению правоохранительного органа или же оператору связи, обслуживающему соответствующие сеансы связи и другие следственные действия.

При рассмотрении данной категории дел можно сделать вывод, что она обладает высокой степенью сокрытия, относится к латентным преступлениям. Причиной проблематики расследования, раскрытия и предупреждения компьютерных преступлений выступает технологический прогресс, обеспечивающий и облегчающий деятельность преступников. Существующие в настоящий момент методики раскрытия и расследования мошенничества с использованием компьютерной информации оказывают незначительное влияние на качество раскрытия и расследования данных преступлений.

Следствием этого выступает снижение количества раскрытых уголовных дел данной категории и отсутствие значимого результата по расследованным и направленным на рассмотрение в суд уголовным делам. Таким образом,

в настоящее время существует необходимость разработки методик с учетом последних достижений в области криминалистики, изменений уголовного и уголовно-процессуального законодательства, а также обязательным содержанием в них научно обоснованных криминалистических рекомендаций относительно методики раскрытия, расследования и судебного разбирательства таких преступлений.

Список литературы

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

2. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельности: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

3. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

4. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Сироткина Дарья Александровна[1]**,**
курсант факультета подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ ИЗ БАНКОМАТОВ

Использование банкоматов стало обычным явлением в современном мире после того, как платежные карты пустили корни в финансовую систему. В России люди впервые увидели банкомат в 1991 г. Он не был подключен ни к одному российскому банку и работал автономно. Только через три года в Москве установили первый полноценно функционирующий банкомат вне отделения банка. Он был запущен в гастрономе «Новоарбатский» в 1994 г. По воспоминаниям очевидцев, люди были сильно удивлены, увидев «ящик с деньгами и без охраны».

При загрузке карточки в картридер человеку предлагается ввести специальный код (ПИН), который присваивается держателю для его идентификации. После этого по каналам связи банкомат соединяется с процессинговым центром своего банка, обрабатывает запрос и открывает доступ к финансовым операциям.

Согласно статистике зарегистрированных и раскрытых преступлений в сфере компьютерной информации и в сфере компьютерных и телекоммуникационных технологий, расследование данных преступлений становится все труднее, поскольку преступники совершенствуют свои способы осуществления противоправной деятельности с использованием банкоматов.

Разновидностями преступных посягательств на банкоматы являются:

1. Взлом сейфа банкомата (также имеет разновидности: взлом сейфа банкомата прямо на месте установки; криминальное вскрытие замка банкомата; кража всего банкомата целиком с последующим вскрытием сейфа в удаленном месте).

Взлом на месте обычно осуществляют с помощью ручного гидравлического инструмента.

Распространенный метод – разрушение сейфового замка. Для этого нужно просверлить в стальной двери сейфа отверстие в строго определенном месте, чтобы после этого попытаться разрушить внутренности замка и открыть дверь [1].

Также используются устройства для подбора кода, отмычки; также в руках преступников могут оказаться действительные коды и ключи от замков, если имеет место сговор.

Для кражи всего банкомата преступники используют физическую силу или автомобиль и стальной трос. После этого его увозят в неизвестном направлении и вскрывают любым доступным способом.

От взлома или кражи в первую очередь применяются технические средства охраны, видеонаблюдение, средства ограничения доступа, крепление банкомата к полу.

Каждый из банкоматов оснащен сигнализацией, выведенной на пульт охраны. Главным предназначением охранной сигнализации банкоматов является оперативная передача тревоги на пульт службы быстрого реагирования. После получения этого сигнала на место срабатывания тревоги выезжает группа, которая предотвращает взлом или хищение банкомата. По статистике, 40 % банковских устройств подвергаются взлому на месте их непосредственной установки. Остальные 60 % сперва похищаются и уже потом вскрываются [2].

В среднем на похищение неукрепленного банкомата без средств физической защиты у злоумышленников уходит в районе 5–10 мин. Служба реагирования добирается на место тревоги от 1 до 30 мин.

Отдельной проблемой является защита сейфовой части банкомата от вскрытия с помощью взрывных устройств. Метод легкого вскрытия сейфа взрывной волной стал популярным среди преступников в последнее время. Обычно для этого используют взрывоопасный газ, который закачивают в сейф, предварительно взломав шаттер (заслонку) устройства выдачи наличных. Для того, чтобы защитить свои банкоматы от таких атак, банк начал установку газоанализаторов в сейфовую часть устройств. Их функционал – определять предельно допустимые концентрации взрывоопасных газов, уменьшать их концентрацию, подавать сигнал тревоги на пульт охраны, включать звуковую и (или) световую сигнализацию (сирену).

2. Мошенничество. Самый распространенный метод – скимминг.

Скимминг (англ. *skim* – снимать) – кража данных карты при помощи специального считывающего устройства, которое копирует всю информацию с магнитной полосы карты. ПИН-код мошенники узнают с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах или рядом с ними. После получения всей нужной информации преступники изготавливают копию карты и обналичивают денежные средства клиента.

Кража банковской карты путем ее механической блокировки («Ливанская петля») – преступник прячет в отверстие картоприемника материал, используемый для рентгеновских снимков, и уходит недалеко от банкомата ждать жертву. Когда жертва понимает, что его карточка застряла, преступник предлагает свою помощь, прося сказать ПИН-код карты. Когда жертва понимает, что вернуть карту уже невозможно, и уходит, преступник возвращается и, зная ПИН-код, забирает деньги, хранящиеся на карте.

Другим способом мошенничества является *Cash-trapping* + *RTF* (*transaction reversal fraud*) – мошенничество, связанное с получением наличных средств и одновременным воздействием на корректную работу банкомата таким образом, что в результате в процессинговый центр от АТМ направляется сообщение об отмене операции по выдаче денег. Объектом нападения является не другой клиент; используется карта, выпущенная, как правило, на подставное лицо или обезличенная.

Установка подложных банкоматов. Задача таких устройств: имитировать работу обычного банкомата, но не производить никаких транзакций, а только считывать данные карт и ПИН-коды к ним [3].

3. Киберпреступления. Подобный вид преступлений характеризуется в первую очередь использованием специального программного обеспечения (ПО), которое «ломает» программное обеспечение самого банкомата и заставляет диспенсер выполнять команды преступника. Для таких преступлений преступникам не нужен доступ в сейф банкомата или данные карт клиентов. Напротив, им нужен доступ в верхний кабинет. Примерами таких преступлений являются ограбления с использованием трояна *Backdoor.MSIL.Tyupkin* и так называемые атаки с помощью *blackbox*. В случае использования трояна *Tyupkin* преступники заранее получали доступ к компьютеру банкомата и устанавливали на него вредоносное ПО.

Атаки с использованием *blackbox* – это способ, при котором преступник подключается непосредственно к устройству выдачи наличных через его коммуникационный интерфейс и получает возможность управлять им со своего ноутбука. Защитой от подобных атак является шифрование канала связи диспенсер – компьютер.

Анализируя судебную практику, можно сделать вывод о том, что хищение денежных средств с использованием банковских карт квалифицируются по ст.ст. 158 («Кража»), 159 («Мошенничество»), 159.3 («Мошенничество с использованием электронных средств платежа»).

В процессе расследования хищений с использованием банкомата для разрешения целого ряда вопросов возникает необходимость в получении специальных знаний. Одним из важных следственных действий, проводимых по делам о хищениях, является назначение судебных экспертиз.

Среди профилактических мероприятий, направленных на предупреждение хищения денежных средств из банкоматов и с их использованием, следует выделить: беседы сотрудников банка со своими клиентами по вопросам безопасности, а также незамедлительное сообщение в правоохранительные органы о выявленном противоправном деянии и предоставление полной информации для организации дальнейшего расследования данного факта [4].

Таким образом, мы хотим сделать вывод о том, что необходимо бороться с таким видом преступлений, а именно совершенствовать нормативно-правовую базу. Например, если законодательно установить норму об ограниченном месторасположении банкоматов (банки, полиция, суды, прокуратура), значительно уменьшится количество таких посягательств, и они будут своевременно и успешно расследоваться, так как банкоматы будут находиться только в местах, оборудованных камерами.

Список литературы

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

2. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. За-

харов // Информационные технологии в правоохранительной деятельности: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

3. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

4. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Молчанова Татьяна Витальевна[1]**,**
доцент кафедры криминологии
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

РОЛЬ И ЗНАЧЕНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ПРЕДУПРЕЖДЕНИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Современное развитие «количественной криминологии» невозможно без одновременного и связанного развития качественно новых теоретических и технологических исследований. Данного рода исследования, многообразные и высокопрофессиональные, позволили сформироваться значительному количеству научных направлений. В то же время данные, на которые опираются эти исследования, либо основаны на достаточно ограниченной официальной статистике, не дающей возможность проводить полномерный количественно-качественный анализ, либо на альтернативных способах сбора данных о преступлениях (анкетирование, интервьюирование, выборочные исследования и т. д.).

Необходимо отметить что в основе любой правоохранительной деятельности государства должна быть грамотно сформулированная уголовная политика, включающая в себя: знание и понимание того, что происходит с противоправным поведением; сформулированная позиция государства и общества к тем или иным формам криминального поведения; понимание, какими средствами необходимо осуществлять предупреждение преступности (как на уровне общего, специального, индивидуального) для каждого вида преступности, в том числе какими возможностями (прежде всего ресурсными) располагает существующая правоохранительная система.

Понимание и измерение организованной преступности в сфере экономической деятельности в России весьма неопределенно с позиций количественного и качественного изучения. Данное обстоятельство является фактором, ограничивающим возможности противодействия данному виду преступности.

Сегодня не имеется каких-либо достоверных параметров оценки именно этого вида преступности. Статистическое измерение организованной преступности в сфере экономической деятельности основано на различного рода отчетах о преступлениях (официальная статистика), где в качестве квалифицирующего признака указано совершение преступления «в составе организованной преступной группы» или «преступного сообщества». Другие данные показывают ее измерение путем суммирования данных оперативного учета субъектов оперативно-разыскной деятельности. Следует отметить, что организованная преступность в сфере экономической деятельности – это особый вид преступности в ее изучении и измерении, который характеризуется гиперлатентностью. Статические данные, сформированные исключительно на выявленных фактах, указы-

вают на незначительный удельный вес лиц, совершивших преступления в составе организованной группы и преступного сообщества в сфере экономической деятельности.

Степень достоверности информационных источников по изучаемым преступлениям, отдельные проблемы практики выявления и расследования преступлений, совершенных организованной преступной группой и преступным сообществом в сфере экономической деятельности, позволяют утверждать, что использовать только их для измерения, прогнозирования и предупреждения не представляется достоверным, целесообразным и объективным ввиду их ограниченной информативности.

Имеющиеся средства статистического сбора, обработки, анализа данных представлены в разнообразном виде. Определяющими и составляющими, без сомнения, являются *информационные технологии.* В комплексе современных информационных технологий особое место занимают Большие данные (*Big data*).

Данный термин применяется для различных данных, многие из которых характеризуются не только большим объемом, но и вариативностью, высокой скоростью накопления, естественным способом создания и особыми процессами, необходимыми для анализа и статистического вывода.

Совсем недавно большие источники данных стали обрабатываться с целью нахождения взаимосвязей в экономических и социальных системах, где ранее при помощи опросов, экспериментов и этнографических наблюдений выводились заключения и строились всевозможные прогнозные тенденции. Большой объем данных связан с постоянно увеличивающимся числом инструментов для сбора данных (например, ресурсы социальных сетей, мобильные приложения, сенсорные устройства), а также с увеличивающейся возможностью хранить и передавать такие данные, связанной с последними усовершенствованиями накопителей информации и компьютерных сетей.

Из всего многообразия Больших данных мы можем проанализировать огромное количество данных, а в некоторых случаях – обработать все данные, касающиеся того или иного явления, а не полагаться на случайные выборки. «Используя все данные, мы получаем более точный результат и можем увидеть нюансы, недоступные при ограничении небольшим объемом данных. Большие данные дают особенно четкое представление о деталях подкатегорий и сегментов, которые невозможно оценить с помощью выборки»[1].

В настоящее время создаются и формируются электронные учеты, реестры, оптимизируются всевозможные государственные услуги и способы аутентификации человека в них, развивается интернет-банкинг. В государственном регулировании используются облачные информационные сервисы и новые формы коммуникаций государственных органов. Источники документов переводятся из бумажного в цифровой электронно-реестровый вид.

---

[1] Шенбергер В. М., Кукьер К. Большие данные: Революция, которая изменит то, как мы живем, работаем и мыслим. – М.: Манн, Иванов и Фербер, 2014. С. 240.

Применение различных информационных технологий открывает значительные перспективы для предупреждения преступности, в том числе и для организованных ее форм.

Одна из проблем, с которой сталкиваются правоохранительные органы, состоит в том, что многие имеющиеся данные о криминологической обстановке содержатся на документальных носителях и не интегрируются с иными сетевыми базами данных. Это делает практически невозможным оперативное и автоматическое установление преступных социальных связей в онлайн-режиме. В связи с этим главным становится не столько умение строить выборку и выбирать правильный метод изучения, сколько знание того, как собрать и обработать объективные данные о преступности.

В последнее десятилетие в странах, где активно развивается цифровая революция, происходит интенсификация практики использования вычислительных, интеллектуальных и иных параметров для анализа данных при изучении организованной преступности.

Реальное измерение организованной преступности в сфере экономической деятельности входит в новую фазу своего изучения и требует иного теоретического и практического понимания. В связи с этим главной задачей современного изучения преступности является формирование пополняемого в онлайн-режиме глобального банка структурированных и неструктурированных данных по организованной преступности в сфере экономической деятельности. Это также вполне обосновано потребностью изучения и использования Больших данных в криминологическом прогнозировании, а также в теории и практике предупреждения преступности. Неэффективность традиционных методов изучения преступности (статистическое наблюдение и описание такого наблюдения, выявление логических ошибок, допущенных законодателем и, соответственно, правоприменителем) формирует гиперлатентность и механизмы искусственного контроля над преступностью.

Необходимо отметить, что традиционно при изучении оценки состояния организованной преступности используется официальная статистическая отчетность, в том числе и судебная. Судебная и другая отчетность не имеются в достаточном виде, поскольку чаще всего не имеется никакого официального обвинения против рассматриваемых организованных форм преступной деятельности в сфере экономической деятельности.

В связи с этим необходимо использовать экспертные мнения судей, прокуроров, сотрудников полиции, адвокатов, а также свидетелей и других лиц, которые могли бы представить информацию из первоисточника. Необходимо использовать сообщения прессы, научные доклады, неправительственные расследования и другую документацию третьих сторон. Многие из этих источников могут привести к правильному первоисточнику информации или укажут нам на новые направления исследований.

Перечисленные источники помогут нам сформулировать обоснованные гипотезы относительно состояния организованной преступности в сфере экономической деятельности с учетом внедренных и в перспективе используемых в правоохранительной деятельности информационных технологий.

Законодательные инструменты применения информационных технологий содержатся в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., реализуются в мероприятиях программы «Цифровая экономика Российской Федерации». Основные направления обеспечения информационной безопасности в области государственной и общественной безопасности определены Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации № 646 от 5 декабря 2016 г. В отраслевых ведомственных документах обозначается значимость повышения эффективности противодействия преступности, использующей информационные технологии.

Сущенко Екатерина Андреевна[1]**,**
курсант факультета института подготовки
сотрудников для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В современных условиях совершенствования и развития глобальных информационно-телекоммуникационных технологий формирования всемирного информационного пространства, а также в результате неустановленного и неурегулированного единообразного законодательства как на национальном, так и на международном уровне в отношении компьютерных преступлений, связанных с противоправном использованием и применением ЭВМ и телекоммуникационных технологий, правоохранительные органы не были подготовлены в полной мере эффективно и качественно воспрепятствовать противоправным действиям в данной сфере, а именно – киберпреступлениям.

В настоящее время УК РФ не содержит понятие «киберпреступления», вследствие чего необходимо обратиться к научным деятелям.

Один из вариантов определения понятия «киберпреступление» мы можем позаимствовать у ученого Д. Н. Карпова: «киберпреступление – это акт социальной девиации с целью экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [1].

Число преступлений в IT-сфере в 2019 г. выросло более чем в полтора раза. Такие данные обнародовала Генеральная прокуратура Российской Федерации, подведя итоги за 8 месяцев текущего года.

Согласно этим данным, правоохранители выявили 180 153 преступления, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Рост составил 66,8 % [2].

Вместе с тем анализ складывающейся оперативной обстановки, связанной с IT-преступностью, свидетельствует о наличии ряда проблемных вопросов, препятствующих эффективной организации соответствующих направлений оперативно-служебной деятельности органов внутренних дел и требующих скорейшего разрешения.

Сохраняется возможность у лиц, занимающихся преступной деятельностью, избегать идентификации путем использования программных технологий *VPN*, *TOR*, *SSL*, позволяющих менять IP-адрес пользователя сети Интернет, создавать

---

[1] © Сущенко Е. А., 2019.
[2] © Гончар В. В., 2019.

динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров посредством SIP-телефонии.

Применяемые способы шифрования данных на распространенных интернет-сервисах не позволяют устанавливать IP-адреса серверов пользователей, отслеживать их активность, устанавливать данные пользователей. Существующий порядок оформления идентификационных модулей операторами сетей подвижной радиотелефонной связи порождает комплекс проблем, связанных с установлением абонента в процессе раскрытия преступлений.

До настоящего времени не завершен процесс формирования договорно-правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисов, в том числе социальных сетей. Отдельного внимания заслуживает вопрос обеспечения доступа правоохранительных органов к идентификационным сведениям о лицах, совершивших платежные операции посредством банковских и иных платежных систем.

Наиболее распространенными киберпреступлениями являются «Неправомерный доступ к компьютерной информации» (ст. 272 УК РФ), «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273 УК РФ) [3]. Распространение получило «Мошенничество, совершенное с использованием электронных средств платежа» (ст. 159.3 УК РФ). Количество случаев в первом полугодии 2018 г. возросло в 7 раз. Также наиболее часто встречаются следующие преступления: ст. 138 УК РФ («Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»); ст. 158 УК РФ («Кража»); ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»); ст. 242 УК РФ («Незаконные изготовление и оборот порнографических материалов или предметов»); ст. 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно-телекоммуникационных сетей») [4–5].

Одной из проблем в расследовании преступлений является недостаточная подготовленность лиц, которые занимаются расследованием, раскрытием и выявлением компьютерных преступлений.

В статье С. Я. Казанцева «Киберпреступность: факторы риска и проблемы борьбы» был проведен опрос сотрудников правоохранительных органов, согласно которому:

– у 95 % респондентов имеется только юридическое образование; другая дополнительная подготовка ими получена не была, что не может не влиять на качество расследования;

– только 5 % из числа опрошенных имели и образование по специальности «Информатика и вычислительная техника»;

– из числа опрошенных 63 % оценивают свой уровень владения персональным компьютером как уровень «среднего пользователя», 37 % считают, что они обладают знаниями «продвинутого пользователя».

– 79 % опрошенных следователей назвали источником знаний компьютерных технологий самообразование, 21 % – курсы повышения квалификации со-

трудников правоохранительных органов, 5 % – коммерческие курсы или специальное образование.

Большинство следователей и дознавателей отметили, что имеющихся знаний для расследования киберпреступлений недостаточно. По мнению опрошенных, необходимы организация соответствующих семинаров и обучение расследования данных видов преступлений [6].

Большая сложность возникает в вопросах терминологии, определения понятия составных частей ЭВМ, системы ЭВМ и компьютерных сетей, правильного понимания общего режима их функционирования в различных технологических процессах.

Данное обстоятельство приводит к тому, что многие следователи (дознаватели) не могут всесторонне и грамотно разобрать те или иные нормативно правовые документы, связанные с данной сферой преступлений, так как возникают большие проблемы с пониманием специфической терминологии киберпреступлений, вследствие чего могут быть упущены определенные обстоятельства, доказательства, предметы, имеющие большое значение для уголовного дела по какому-либо преступлению данной сферы. Нормативные документы, регламентирующие правовой режим функционирования средств электронно-вычислительной техники и обработки охраняемой законом компьютерной информации, остаются неизвестными и, соответственно, не учитываются в процессе проведения оперативно-разыскных мероприятий и следственных действий, что в конечном счете значительно затрудняет выявление преступлений, сказывается на полном и объективном расследовании уголовных дел данной категории преступлений.

Следующей проблемой расследования киберпреступления является факт несвоевременности.

Это означает, что данные виды преступления отличаются своей латентностью, т. е. достаточно сложно установить лицо, совершившее преступление, место совершения преступления, время и т. п., так как преступление может быть совершено в одно время, а информация о факте совершения преступления может поступить в правоохранительные органы лишь через какое-то время. Также мы можем установить тот факт, что при обнаружении данного преступления мы сталкиваемся с общественно опасным последствием, т. е. общественно опасным действием как основным признаком объективной стороны, которое трудно установить.

В 53 % случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней. Несвоевременность выявления преступлений отметили 75 % опрошенных следователей [7].

Несомненно, запоздалое начало предварительного расследования может привести к полной утрате необходимых доказательств, увеличению сроков предварительного расследования и другим негативным последствиям. По общему правилу, несвоевременное выявление киберпреступлений влечет за собой опасность уничтожения следов совершенного преступления, которые необходимы для дальнейшего уголовного судопроизводства [8].

Еще одной проблемой является установление факта совершения преступления или непосредственно сам состав преступления, поскольку данные преступ-

ления могут совершаться абсолютно из любой точки мира – как из дома, так и из-за границы. Также в качестве примера приведем ситуацию, связанную с незаконной группой лиц в сети Интернет («Синий Кит»). В данном расследовании не удалось установить субъект преступления, так как все контакты вели в Латвию. Это действительно существенно усложняет процесс расследования преступления и установления факта совершения преступления. Статистика 2018 г. охватывает период с ноября 2017 по октябрь 2018 гг. *Kaspersky Security Network* приводит следующие цифры:

– решения «Лаборатории Касперского» отразили 1 876 998 691 атаку, проводившуюся с интернет-ресурсов, размещенных в различных странах мира;

– зафиксирован 554 159 621 уникальный *URL*, на которых происходило срабатывание веб-антивируса;

– веб-антивирусом зафиксированы 21 643 946 уникальных вредоносных объектов;

– атаки шифровальщиков отражены на компьютерах 765 538 уникальных пользователей;

– за отчетный период майнерами были атакованы 5 638 828 уникальных пользователей;

– попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах 830 135 пользователей [9].

По данным Генеральной прокуратуры Российской Федерации, за весь 2017 г. в стране были зафиксированы 90 587 киберпреступлений. За первые восемь месяцев 2019 г. в России были зарегистрировани 180 153 киберпреступления [10].

Вследствие данных показателей мы можем сделать вывод о том, что киберпреступления, зафиксированные «Лабораторией Касперского», и преступления, зафиксированные Генеральной прокуратурой Российской Федерации, максимально расходятся по количеству – данный факт означает, что правоохранительные органы не способны в полной мере обеспечить противодействие кибератакам, а также расследованию, раскрытию и выявлению данных преступлений. Одной из проблем данного факта является то, что очень сложно установить факт совершения преступления.

Следующей проблемой расследования киберпреступлений является проблема проведения некоторых следственных действий.

Чаще всего проводятся следующие следственные действия: осмотр места происшествия, допрос, обыск, выемка, значение судебных экспертиз.

Примером проблемы проведения следственного действия может послужить осмотр места происшествия, так как само место происшествия (преступления) практически невозможно установить, поскольку противоправные действия могли совершаться из любой точки мира.

Еще одним примером проблемы применения следственных действий может послужить назначение судебных экспертиз. Поскольку для их назначения следователю необходимо поставить ряд вопросов эксперту для установления того или иного факта совершения преступления, от этого будет завесить результат

экспертиз. Но вследствие недостаточной компетенции и знания следователя в предметной области, связанной с ЭВМ и телекоммуникационными устройствами, вопросы могут быть неисчерпывающими, неграмотно поставленными, что приведет к потере каких-либо доказательств, важных для расследования и раскрытия преступлений [11].

Раскрытие и расследование киберпреступлений остается довольно трудной задачей для большинства сотрудников правоохранительных органов [12], что отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Список литературы

1. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – Т. 22. – № 8. – С. 46–50.

2. «Уголовный кодекс Российской Федерации» от 13 июня 1996 г. №63-ФЗ (ред. от 12.11.2018) // Собр. законодательства Рос. Федерации. – 1996. – 17 июня. – № 25. – Ст. 2954.

3. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Отчет Генеральной прокуратуры Российской Федерации. – 2018. – 14 авг.

4. Шевченко Н. Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Текст научной статьи по специальности «Право».

5. Киберпреступления: основные проблемы расследований [Электронный ресурс] // Институт судебных экспертиз и криминалистики. – URL: https://www.klerk.ru/law/articles/431376 (дата обращения: 05.11.2019).

6. Kaspersky Security Network [Электронный ресурс] // URL: https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906 (дата обращения: 10.11.19).

7. Данные Генеральной прокуратуры Российской Федерации [Электронный ресурс] // URL: http://www.tadviser.ru/index.php (дата обращения: 10.11.19).

8. В России резко выросло число преступлений в IT-сфере [Электронный ресурс] // URL: https://rg.ru/2019/09/27/v-rossii-rezko-vyroslo-chislo-prestuplenij-v-it-sfere.html (дата обращения: 05.11.2019).

9. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

10. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельно-

сти: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

11. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

12. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Тараканова Татьяна Эдуардовна[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Поликарпов Евгений Сергеевич[2]***,***
доцент кафедры специальных информационных технологий УНК ИТ,
кандидат технических наук

ОБЗОР СОВРЕМЕННЫХ ИСТОЧНИКОВ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Информационно-коммуникационные технологии все шире используются в повседневной жизни, в медицине, здравоохранении, образовании и науке, органы государственной власти все чаще используют их для организации эффективного управления и повышения качества услуг, предоставляемых населению.

Сегодня сбор информации из открытых источников в значительной степени направлен на информационное пространство, поскольку все больше информации становится доступной в электронном виде, особенно при развитии сети Интернет. Пользователи сети Интернет ежедневно генерируют петабайты данных. Миллионы пользователей получают доступ к миллиардам веб-страниц каждые миллисекунды, создавая сотни записей в журналах серверов каждым нажатием клавиши и щелчком мыши.

Кроме того, появление интернет-торговли, социальных медиа вынуждает пользователей оставлять в сети огромное количество персональных данных. Основываясь на этих фактах, можно с уверенность сказать, что информация, циркулирующая в сети Интернет, является лакомым кусочком для разведывательных служб.

Для получения оперативно значимой информации о физических лицах, о фактах и обстоятельствах, имеющих значение для решения задач оперативно-разыскной деятельности, может проводиться сбор информации о злоумышленнике из открытых источников в сети Интернет (*OSINT*): его образ жизни, адрес, родственные и дружеские связи, наличие недвижимости, регистрация по месту жительства, принадлежность телефонных номеров, информация о владельце транспортного средства, криминальная история, выдача документов, удостоверяющих личность, и служебных удостоверений, наличие оружия и др. [6].

В настоящее время в открытом доступе имеется большое количество программ, которые помогают найти информацию о человеке в сети Интернет.

Источником получения информации выступает мессенджер *Telegram*. С помощью ботов мы можем получить различную информацию об интересующем нас лице:

– *@egrul_bot*. Данный бот пробивает конторы и индивидуальных предпринимателей. По вводу ФИО или названия фирмы предоставляет ИНН объекта;

учредителей бизнеса и партнеров, отчет, налоговую декларацию. И наоборот: поиск по ИНН выдаст ФИО или конторы;

– *@get_kontakt_bot*. Бот пробивает номер мобильного телефона, а именно то, как записан запрашиваемый контакт в разных телефонных книжках ваших товарищей, подруг, коллег;

– *@SmartSearchBot* поможет Вам найти дополнительную информацию относительно телефонного номера, *ID* в социальной сети «ВКонтакте», электронную почту или ИНН юридического или физического лица;

– *@AvinfoBot*. Бот, который по вводу мобильного телефона выдаст номер и марку машины, а также ссылку и все объявления на *Avito.ru*.

Еще одним источником является *Creepy* – инструмент *OSINT* для геолокации, предназначенный для сбора геолокационной информации о пользователе на основе данных его аккаунтов *Twitter*, *Instagram*, *Google+* и *Flickr*. Достоинство этого инструмента – он штатно входит в *Kali Linux*.

Информацию по фотографии можно получить с помощью *Social Mapper* – программы с открытым исходным кодом, предназначенной для обнаружения лиц и для изучения их страниц в социальных сетях. Программа использует автоматические методы для поиска на сайтах социальных сетей по именам и изображениям целей, чтобы точно идентифицировать и сгруппировать присутствие человека, выводя результаты в наглядный отчет, который оператор-человек может быстро просмотреть.

Если рассмотреть практическое применение для правоохранительных органов, данная программа является источником оперативно значимой информации в информационном пространстве, выдает в результате страницы пользователей, которые когда-либо выкладывали фотографии с интересующим нас человеком, т. е. можно изучить родственные, дружеские либо преступные связи. *Social Mapper* поддерживает следующие платформы социальных сетей: *LinkedIn*, *Facebook*, *Twitter*, *Google+*, *Instagram*, «ВКонтакте», *Weibo*, *Douban*.

Существует сервис – *knowem*, который умеет проверять регистрационные данные более 400 различных социальных сервисов и более 40 доменных имен (в окончательной выдаче они разделены на 16 категорий). При вводе необходимого ника нам высвечивается ссылка на его страницу в социальной сети. Данный сервис находится в открытом доступе.

SpiderFoot обрабатывает одновременно более 100 открытых источников; доступна расширенная настройка. Также есть фильтр по кейсам: поиск всевозможной информации о человеке, поиск цифровых следов с помощью поисковых роботов и поисковиков, черные списки и другие открытые источники для проверки на вредоносность и сбора информации. Последний фильтр лучше всего подходит для расследования.

SpiderFoot – утилита, предназначенная для автоматизации сбора разведывательной информации о цели (представленной IP-адресом или доменным именем). В отличие от своего аналога *Maltego*, интерфейс *SpiderFoot* доступен в браузере.

С помощью данной программы мы получаем отображение графа с визуальным представлением результата сканирования, где множество зависимостей – это сайты, где был замечен пользователь.

Для анализа данных, которые собираются в офлайн-режиме, а не из открытых источников, необходимо использовать *CaseFile*.

Аналитические инструменты *Recorded Future* помогают выявить тенденции в больших объемах неструктурированной информации, извлекая необходимые факты из сети Интернет. Используя специальные алгоритмы, этот сервис создает графики с визуализацией трендов в прошлом, настоящем и в будущем.

Утилита *Trape* представляет собой инструмент, позволяющий отслеживать человека. Данный инструмент запрашивает ссылку-приманку, которая отслеживается в сгенерированной контрольной панели. Именно контрольная панель и является самым интересным. В ней есть подробная информация о том, сколько людей переходило по ссылке, количество кликов, а также подробная информация о сети устройства и его местоположении.

Сам инструмент скорее образовательный, так как полученная ссылка не скрывается (даже в сервисе сокращения).

Кроме того, требуются токены *API Google Maps* и *ngrok*. Инструмент создан только в научных целях, и для полного использования требуется согласие обеих сторон.

Spokeo – это программа, позволяющая анализировать данные из различных источников, таких как телефонные книги, фотоальбомы, социальные сети, маркетинговые опросы, данные государственной переписки населения и многое другое. Также показываются и демографические данные, социальные профили, анализируется оценка финансового положения и права собственности.

Сайт *Kartoteka.ru* дает уникальную возможность проверить и проанализировать любую компанию, зарегистрированную на территории Российской Федерации.

Данный сервис поможет быстро и качественно произвести анализ компании, оценить ее кредитоспособность, размеры бизнеса, ее связи и риски. В соответствии с законодательством Российской Федерации нам предоставляются только правдивые сведения об участниках российского бизнеса, а также создаются удобные ресурсы и инструменты для размещения информации заинтересованными лицами.

Рассмотрим способы изучения социальных сетей в целях получения оперативно значимой информации.

Наиболее востребованным методом в изучении социальных сетей считается опрос. Опрос бывает анкетным, телефонным, при помощи сети Интернет и в виде интервью, которое бывает формализованным и неформализованным [5]. Главным отличительным признаком от традиционного опроса является содержание инструментария исследования. Бланки анкет или интервью представляют собой небольшое количество вопросов. Кроме того, пользуясь методом опроса, исследователь в большей степени изучает презентацию социальной сети, в которой показывает субъективное восприятие автора, определенное состоянием его памяти и многими другими факторами, не поддающимися анализу. Данный

метод сбора данных, как включенное наблюдение, не получил большего применения в исследовании социальных сетей, хотя, казалось бы, давал уникальную возможность изучить процессуальную сторону социальной жизни.

Следующим по популярности методом сбора данных в исследовании социальных сетей является анализ документов. Изучение разного рода документальных архивов, таких как архивные записи, статьи из газет и журналов, произведения истории и литературы, следственных материалов и многое другое, дает исключительную возможность получения разнообразного рода информации о социальных отношениях и связях индивида.

Таким образом, на основе анализа открытых источников в сети Интернет должны использоваться специальные программы поиска и анализа данных. Для удобства изучения материала и технологий, применяемых в *OSINT*, мы рассмотрели некоторые инструменты сбора информации в сети Интернет. На сегодняшний день все больше распространяется *SOCMINT* – это подраздел *OSINT*, фокусирующийся на сборе и мониторинге данных в социальных сетях, так как сейчас почти не осталось людей, которые не зарегистрированы ни в одной социальной сети.

Список литературы

1. Конституция Российской Федерации [Электронный ресурс] : принята всенародным голосованием 12 декабря 1993 г. // СПС «Консультант Плюс». – URL: https://www.consultant.ru.

2. Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

3. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Бирюков А. А. Информационная безопасность: Защита и нападение. – 2-е изд., перераб. и доп. – М. : ДМК Пресс, 2017.

5. Введенская О. Ю. Особенности следообразования при совершении преступления посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4. – С. 210.

6. Камский В. А. Защита личной информации в Интернете, смартфоне и компьютере. – СПб. : Наука и Техника, 2017.

7. Сергеев А. Н. Администрирование сетей на основе Windows : лабораторный практикум [Электронный ресурс] / А. Н. Сергеев, Е. В. Татьянич. – Волгоград : Волгоградский государственный социально-педагогический университет, 2017. – 48 с. – URL: http://www.iprbookshop.ru/62772.html. – ЭБС «IPRbooks».

8. Шаньгин В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин – Саратов : Профобразование, 2017.– 702 с. – URL: http://www.iprbookshop.ru/63594.html. – ЭБС «IPRbooks».

9. Дуленко В. А. Преступления в сфере высоких технологий : учебное пособие / В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков. – М. : ЦОКР МВД России, 2010.

10. Защита от вторжений: расследование компьютерных преступлений [Электронный ресурс] / К. Мандиа // URL: http://computersbooks.net/index.php?id1=4&category=rukovodstvo-po-po&author=mandia-k&book=2005.

11. Маркин Ю. В. Обзор современных инструментов анализа сетевого трафика [Электронный ресурс] / Ю. В. Маркин, А. С. Санаров // URL: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf.

12. Коммерсантъ Картотека [Электронный ресурс] / URL: https://www.kartoteka.ru.

Ткачева Виолетта Дмитриевна[1]*,*
курсант 383 учебного взвода института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Гончар Владимир Владимирович[2]*,*
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ПРАВОВОЕ РЕГУЛИРОВАНИЕ И НЕЗАКОННЫЕ ДЕЙСТВИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

В эпоху глобальных цифровых изменений защита всех элементов современных систем становится вопросом невероятной важности. Для ее обеспечения необходимы не только мощные внутренние структуры, но и эффективное международное сотрудничество. В таких рамках открытость, готовность делиться информацией о потенциальных угрозах и случаях успешных атак помогают делать правильные выводы и работать на результат.

Именно область правового регулирования является одной из главных идей сегодняшней статьи.

Где международные законы в области интернет-безопасности? Одни государства предлагают заключать договоры, обязательные на международном уровне, другие продвигают региональные нормативные акты; между тем количество выявленных органами внутренних дел Российской Федерации преступлений в сфере информационных технологий ежегодно увеличивается в 1,8–2 раза. Если в 1997 г. были выявлены только 17 преступлений такого рода, то по данным 2003 г. их число превысило 10 000.

В 1997 г. в Российской Федерации была введена уголовная ответственность за преступления в сфере компьютерной информации, а в 1998 г. – в МВД России создано специальное подразделение по борьбе с преступлениями в сфере информационных технологий [1–2].

Тем не менее уровень участия в международном правотворчестве по вопросам безопасности в интернет-структуре остается низким [3–4]. Похоже, мировое сообщество не получило толчок такой силы, чтобы сплотиться для противодействия реальной и крайне серьезной опасности. Чтобы прийти к соглашению по данной проблеме, у нас остается все меньше времени. Для борьбы с данным видом преступности нужны независимые от государств глобальные структуры, которые будут принимать и применять международные законы по интернет-безопасности, в том числе устанавливать «стандарты» атак и определять меры наказания для преступников.

В мире насчитываются более 5 млрд пользователей мобильных телефонов, более 4 млрд интернет-пользователей, более 3 млрд пользователей социальных сетей.

Текущая ситуация в правовом мире осложняется тем, что не во всех странах хакерство считается преступлением. Различия в культуре, менталитете и приоритетах делают выработку международных норм еще более трудной задачей. Однако именно создание таких законов станет следующим серьезным шагом на пути к победе над преступностью в области интернет-регулирования.

Есть два подхода к организации безопасности: один основан на требованиях к системе безопасности, второй – на управлении ими.

При внедрении технологий защиты часто не учитывают особенности бизнеса и IT-инфраструктуры, что приводит к неэффективной защите: средства есть, персонал есть, а безопасность остается на низком уровне. Чтобы избежать подобных ситуаций, необходим подход, при котором безопасность выстраивается с учетом особенностей организации и использует технологии безопасности и информационные технологии.

Уровень зрелости интернет-безопасности не может быть выше уровня IT-зрелости. Базовые IT-процессы – фундамент для эффективных систем управления как IT-инфраструктурой, так и безопасностью в интернет-сфере.

Ответственность за незаконные действия в интернет-пространстве

Среди особенностей преступлений в сети Интернет можно также выделить возраст: 16,3 % – это лица до 18 лет, 58,9 % – от 18 до 25 лет. Свыше 75 % выявленных преступников составляет молодежь. Следует отметить, что 67 % от общего числа правонарушителей имеют высшее или неоконченное высшее образование, что говорит о высоком интеллектуальном уровне противодействующей стороны. Часто профессиональные преступники в интернет-сфере объединяются в группы.

Сбербанк России сообщил, что в 2019 г. на мировом уровне ущерб компаний от кибератак увеличился в 1,6 раза по сравнению с прошлым годом. По данным банка, в 2018 г. убытки компаний составили 1,5 трлн долларов, в этом году они достигли 2,5 трлн долларов.

«К 2022 г., по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак вырастет до 8 трлн долларов». Мы считаем, что данные цифры не могут не заставить задуматься об ужесточении ответственности за данные преступления.

Что касается международного регулирования данной проблемы, предположим, что государства согласны с правилами использования «интернет-оружия» – например, не атаковать критически важную инфраструктуру в мирное время. Что происходит, когда государство нарушает одно из этих правил, – можно ли определить в этом случае ответственное лицо? Используемые и обсуждаемые правоприменительные методы включают дипломатические заявления, угрозы и экономические санкции. Такие методы дают незначительные результаты.

Исполнительный вице-президент Института «Восток – Запад» Б. Макконнел описал один из возможных режимов контроля, который позволит повысить безопасность и установить стабильность в киберпространстве.

Увеличивая стоимость кибератак, компании делают их невыгодными для преступников. Добиться этого можно следующими способами:

– сканировать клиентские устройства и требовать улучшения их безопасности;

– распространять доказательства атрибуции атак;
– блокировать трафик, идущий от атакующего.

Однако подобные действия со стороны организаций могут привести к удорожанию их услуг и издержкам репутации. Сотрудничество с государством в этих вопросах поможет минимизировать масштаб негативных последствий.

Атаки становятся все более продвинутыми и сложными для определения. Киберпреступники могут месяцами находиться в IT-инфраструктуре компании и оставаться незамеченными. Такие атаки наносят колоссальный ущерб – особенно когда речь идет об объектах критической инфраструктуры. Необходимо совершенствовать устаревшие системы, внедрять новые методы защиты и активно обмениваться информацией об угрозах с другими организациями.

Таким образом, можно сделать вывод о необходимости регулирования в сфере информационных технологий не только со стороны конкретного государства, но и по части международного сотрудничества. Только созданием совместных (международных) правовых актов можно привлечь к ответственности преступников и пресекать их действия.

Помимо этого, государство должно защищать права граждан в киберпространстве, повышать уровень цифровой чистоты населения: успех многих кибератак напрямую связан с неподготовленностью пользователей.

Список литературы

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

2. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельности: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

3. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18–27.

4. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

Цимбал Виталий Николаевич[1],
старший преподаватель кафедры информационной безопасности
Краснодарского университета МВД России,
кандидат юридических наук

АНАЛИЗ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРИМЕНЯЕМЫХ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ

Благодаря отсутствию различной отчетности, делопроизводства, необходимости соблюдать правила и законы (не считая «законов» субкультуры) преступники могут использовать и используют в своей противоправной деятельности новые, более современные и эффективные информационные технологии.

Правоохранительные органы зачастую выступают в «роли» отстающих, так как законные процедуры закупки, постановки на снабжение им дальнейшее использование новейших достижений науки и техники являются сложными, долгими и, к сожалению, не всегда эффективными. Хотя о необходимости и обязанности использования обозначенного выше говорится в Федеральном законе от 07 февраля 2011 г. № 3-ФЗ «О полиции», в частности, в ст. 11.

Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов [1].

Приемы и соответствующие технологии, применяемые злоумышленниками, следующие:

1. Наиболее опасным приемом, который в последнее время получил достаточно большую популярность в криминальной среде, является социальная инженерия. У ученых данный феномен также вызывает научный интерес, и изучается она как современное явление, способ совершения преступлений, так же, как некоторая возможность изучения психологии жертвы и социальных явлений.

В. В. Суворова, Л. А. Суворова формулируют следующее определение социальной инженерии: «…вид совершения компьютерных преступлений, направленный на несанкционированное получение информации путем использования слабых мест в психике человека» [2, с. 73]. А. В. Кравченко видит рассматриваемый термин с точки зрения психологии: «…набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушению устоявшихся правил и политик в области информационной безопасности» [3, с. 48]. А. Г. Окуловская и И. Е. Филиппов дают более емкое определение: «…метод несанкционированного доступа к информации или системам хранения информации без использования технических средств, основанный на определенной совокупности приемов, методов и технологий (используются слабости человека и человеческий фактор) прикладных наук (психология, социология и т. п.), позволяющих

создать такое пространство, условия и обстоятельства, которые максимально эффективно позволяют добиться результата от цели атаки» [4, с. 38].

Мы согласимся с обозначенным определением частично и отметим, что преступники довольно искусно применяют методы психологии, иногда задают жертвам неожиданные вопросы, постоянно поддерживают беседу, тем самым отвлекая потерпевшего и не давая ему обдумать сказанное; в некоторых случаях перед телефонным звонком и (или) направлением электронного письма собирают информацию об объекте противоправного деяния: установочную (ФИО, город проживания, возраст и т. д.), семейное положение, обслуживаемая кредитная организация, интернет-провайдер и иное, для обнаружения подобного необходимо использование информационных технологий (открытые данные в сети Интернет, различные базы и банки данных). Объем и количество подобных сведений зависят от способа совершения преступления и имеющейся в распоряжении злоумышленников информации о жертве. Нельзя не признать тот факт, что многие преступники – отличные ораторы и тонкие психологи.

Способов социальной инженерии большое количество: фишинг, фарминг, фрикинг, претекстинг, применение совместно с классическими методами программного обеспечения (как правило, вредоносного), обратная социальная инженерия и т. д. [4, с. 39–41; 5, с. 26–27; 6, с 22–23; 7, с. 2–4].

2. Информационно-телекоммуникационная сеть Интернет и ее возможности. Как известно, обозначенный ресурс выступает и отличным местом для общения через социальные сети, тематические форумы, сайты, всевозможные хостинги (фото – *Instagram*, видео – *YouTube*), новостные агрегаторы («Яндекс.Дзен», «Пульс» от *Mail.ru*), и площадкой для совершения огромного количества разнообразных противоправных деяний. Популярность сети Интернет для обозначенного состоит не только в его возможностях вообще, но и в доступности – как к его ресурсам, так и к технике (смартфон, планшетный компьютер, бесплатные точки доступа *Wi-Fi*), благодаря которой происходит подключение.

По последним данным, общее количество пользователей на январь 2019 г. составило порядка 4,3 млрд человек. Активными пользователями социальных сетей являются 3,4 млрд – это немногим менее половины всего населения нашей планеты, которое составляет свыше 7,6 млрд человек [8].

Схематично сеть Интернет делится на несколько частей:

– открытая – среда, которую использует подавляющее большинство людей, так называемый *TheSurfaceWeb* («Поверхностная сеть»). При этом от общей массы всех ресурсов и информации, имеющейся во Всемирной паутине вообще, это всего лишь 4 процента. К данной части относятся и всем известные поисковые системы (*Google*, «Яндекс», *Bing*, *Mail.ru*), социальные сети («ВКонтакте», *Facebook*), различные хостинги (*YouTube*, *Instagram*) и т. п.;

– следующая часть является неиндексируемой поисковыми системами, также называемая *DeepWeb* («Глубинная сеть») – это примерно 90 % от общего объема сети Интернет. В ней располагается финансовая информация, репозитории различных организаций, специализированные форумы и иные ресурсы, попасть в которые можно по приглашению, зная электронный адрес и т. д.;

– заключительной частью Всемирной сети является *DarkWeb*, или *DarkNet* («Темная сеть»), доступ к такому ресурсу получить обычными способами (имея компьютер, браузер и соединение с сетью) невозможно. Подключение осуществляется путем применения специфических технологий – протоколов *I2P* и *TOR*, благодаря этому вся работа в рассматриваемой сети полностью анонимна.

Протокол *I2P* (англ. *Invisible Internet Project*) является децентрализованной анонимной оверлейной сетью, которая при передаче информации между узлами сети использует шифрование. Также к особенностям данной технологии можно отнести необходимость использования специализированных программ для установления криптографически защищенного соединения и веб-браузера.

Протокол *TOR* (*The Onion Router*) обеспечивает анонимность путем использования промежуточных узлов между клиентским приложением и сервисом, к которому пользователь получает доступ, т. е. идентифицировать пользователя по IP-адресу невозможно [9, с. 217].

Интересным является и наличие в *DarkNet* возможности осуществления финансовых операций. Злоумышленники используют криптовалюту и, соответственно, специфические кошельки, отследить движение денежных средств при этом практически невозможно, как и установить личность и номера счетов контрагентов.

Используются изучаемые ресурсы для продажи наркотических средств, оружия, поддельных документов, получения всевозможных услуг (хакеров и даже киллеров), распространение запрещенного контента и т. п.

3. Мессенджеры, например, *Telegram*, который получил в последнее время большую популярность в связи с его анонимностью (которая достигается использованием сквозного шифрования), существованию секретных каналов, полному отсутствию сотрудничества с правоохранительными органами нашего государства.

Представители мессенджера утверждают, что ключи шифрования передать органам исполнительной власти невозможно в связи со спецификой архитектуры *Telegram* [10].

Основная противоправная деятельность в *Telegram* – это пропаганда употребления наркотиков и их распространение. С использованием тематических каналов, посвященных обороту наркотиков, пропагандируется употребление наркотических веществ, рекламируются интернет-магазины и чат-боты, специализирующиеся на торговле наркотиками, происходит вовлечение подростков и молодежи в деятельность, направленную на сбыт наркотиков [11, с. 8]; также осуществляется руководство преступными группами, которые могут насчитывать до 15 отдельных подгрупп участников.

Однако вышеобозначенное не является исчерпывающим перечнем преступлений, совершаемых при помощи *Telegram*: в последнее время все чаще появляется информация от официальных представителей правоохранительных органов, что при задержании ячейки террористов обнаруживается факт их общения в мессенджере [12] либо подготовка террористических актов осуществлялась с использованием *Telegram* [13] и т. д.

На сегодняшний день в Российской Федерации данный мессенджер продолжают блокировать, занимается этим Роскомнадзор.

Помимо рассмотренного нами мессенджера на рынке существуют и иные коммерческие продукты, позволяющие предоставлять аналогичный функционал, например: *Threema, Wickr, Signal, CoyIM* и другие, но по популярности с *Telegram* они в ближайшее время вряд ли сравнятся.

4. Вредоносные программы представляют собой серьезную угрозу. К таким относятся компьютерные вирусы, троянские программы, сетевые черви и многое другое. По своему функционалу они могут незаметно проникать на компьютер пользователя, отслеживать его действия в сети, копировать конфиденциальные данные, осуществлять управление оборудованием и иные незаконные действия.

Довольно ярким случаем представляется следующий. 12 мая 2017 г. в сети Интернет появился троян-шифровальщик *WannaCry*. Только за один день им было заражено более 300 тыс. компьютеров. Больше всего атак пришлось на Россию, также серьезно пострадали Украина, Индия, Тайвань, всего программа была обнаружена в 74 странах [14]. Целью использования подобной программы является вымогательство денежных средств у жертвы под угрозой оставления пользовательских данных в зашифрованном виде.

К сожалению, такие случаи нередки. Как нами говорилось в начале данной работы, современная преступность очень быстро осваивает новые технологии, умело их применяет, виртуозно совмещая при этом и психологию, и программирование, и социологию, и несовершенство законодательства и т. п.

Нет причин сомневаться, что правоохранительным органам придется столкнуться с разнообразными противоправными деяниями, которые будут совершаться как при помощи современных информационных технологий, так и посредством них. Совершенствование методик выявления, разработка новых способов борьбы с преступностью и включение в арсенал правоохранителей знания и новейших достижений науки и техники можно назвать ключом к победе над преступностью.

Список литературы

1. Федеральный закон от 27 июня 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс». – URL: https://www.consultant.ru.

2. Суворова В. В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В. В. Суворова, Л. А. Суворова // Теория и практика приоритетных научных исследований : сборник научных трудов VIII Международной научно-практической конференции. – Смоленск, 2019. – С. 71–74.

3. Кравченко А. В. Психологические механизмы социальной инженерии при совершении преступлений // Журнал психологии и педагогики служебной деятельности. – № 1. – 2019. – С. 46–50.

4. Окуловская А. Г. Социальная инженерия: определение, техники атаки, способы защиты / А. Г. Окуловская, И. Е. Филиппов // Сборник статей III Международной научно-практической конференции «Инновационное развитие науки и образования». – Пенза : Наука и Просвещение, 2018. – С. 38–42.

5. Тепляков С. П. Социальная инженерия: Анализ и методы защиты / С. П. Тепляков, А. С. Тимохович // Academy. – 2018. – № 7 (34). – С. 26–27.

6. Ламинина О. Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. – 2017. – № 2. – С. 21–23.

7. Балакин К. А. Социальная инженерия: вчера, сегодня, завтра // Политехнический молодежный журнал. – 2019. – № 6 (35). – С. 1–8.

8. Digital 2019: Global Internet Use Accelerates [Электронный ресурс] // URL: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (дата обращения: 15.10.2019).

9. Фролов А. А. Исследование механизмов распространения, запрещенного содержимого в Darknet / А. А. Фролов, Д. С. Сильнов // Современные информационные технологии и ИТ-образование. – 2017. – № 4. – С. 216–224.

10. Сайт РБК [Электронный ресурс] // URL: https://www.rbk.ru/technology_and_media/02/04/2018.

11. Сайт РБК [Электронный ресурс] // URL: 5ac1f2f89a79471b98083b34 (дата обращения: 16.10.2019).

12. Суходолов А. П. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Telegram» в распространении наркотиков / А. П. Суходолов // Всероссийский криминологический журнал. – Т. 13. – № 1. – С. 5–17.

13. Сайт РБК [Электронный ресурс] // URL: https://www.rbk.ru/society/27/04/2018/5ae3093b9a79476c2f777ee8 (дата обращения: 16.10.2019).

14. Сайт «Московский Комсомолец» [Электронный ресурс] // URL: https://www.mk.ru/politics/2017/06/26/fsb-terroristy-ispolzovali-telegram-pered-vzryvom-v-metro-peterburga.html (дата обращения: 16.10.2019).

15. Kasperski Daily [Электронный ресурс] // URL: https://www.kaspersky.ru/blog/wannacry-ransomware/16147 (дата обращения: 17.10.2019).

Шорникова Валентина Сергеевна[1],
курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я Кикотя

Гончар Владимир Владимирович[2],
заместитель начальника кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПОМОЩЬЮ СКИММИНГОВОГО ОБОРУДОВАНИЯ

В настоящее время большие обороты набирает уплата за счет безналичных средств, т. е. с помощью банковских карт. В связи с этим появляются новые преступления в сфере нарушения законодательства безналичных расчетов. Злоумышленники пытаются получить средства граждан с банковских карт различными способами. Одним из таких способов является скимминг, что представляет собой (англ. *skim* – снимать сливки) установку на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты. Скиммеры устанавливаются «в приемник банкомата для считывания информации с магнитной полосы, получения ПИН-кода и других данных с целью их дальнейшего использования для изготовления поддельной пластиковой карты и хищения денежных средств» [1]. Установленное оборудование может накапливать украденную информацию о пластиковых картах либо дистанционно передавать ее по радиоканалу злоумышленникам, находящимся поблизости.

Скиммеры различаются по способу передачи информации злоумышленникам: накапливают украденную информацию (мошенник считывает данные после снятия оборудования); дистанционно передают ее по радиоканалу.

Во многих случаях скимминг-оборудование представляет собой два типа накладок, конструкция и цветовая гамма которых не всегда соответствует индивидуальным особенностям банкоматов, на которых их планируется размещать (*рис. 1*).

Рис. 1. Скимминг-оборудование и его содержимое

Впервые нештатное оборудование на банкомате Сбербанка России, идентифицированное как скимминг, было обнаружено в 2002 г. [2] Данное устройство выглядело как достаточно громоздкое сооружение, имитирующее лицевую панель банкомата. Монтировалось оно в течение нескольких минут, требовало точной настройки и частой перезарядки. В результате неточных действий установщика навесная конструкция нередко отваливалась в момент проведения операции. Современные технологии скимминга импортированы в Россию из-за рубежа. В большинстве случаев скимминг-оборудование представляет собой достаточно компактное, насыщенное электронными компонентами штатное или имитирующее штатное навесное оборудование (пассивные антискимминговые накладки на картридере или заглушки, закрывающие технологические отверстия банкомата), различного рода накладки, закамуфлированные под корпоративные цвета банка – владельца банкомата, задача которых получить персональные данные банковской карточки. Нештатное оборудование может быть как двухкомпонентным, т. е. состоять из двух элементов: накладки на картридер и планки с видеокамерой или накладной клавиатуры, так и однокомпонентным, совмещающим в себе считыватель магнитной полосы и накопитель ПИН-кодов.

Исходя из этого, при осмотре банкомата следует обращать внимание на следующее:

– частично закрытые стикеры, штатно размещенные на банкомате, в результате чего текст на них становится трудночитаемым;

– скимминговые накладки, которые могут частично или полностью закрывать технологические отверстия банкомата (в данном случае прикрыто отверстие в/к, контролирующей получение клиентом денег);

– неестественно выступающие, а также нависающие части нештатных накладок над клавиатурой, экраном монитора или находящиеся на корпусе банкомата, в том числе на боковых поверхностях;

– наличие неестественных теней под плафоном штатного светильника банкомата;

– различающийся цветовой тон на различных элементах лицевой панели банкомата;

– провода, проходящие по лицевой панели банкомата;

– различного рода загрязнения, под которыми могут скрываться элементы крепления скимминга.

Особую опасность представляют скиммеры нового поколения. [3] Их главный признак – большая длина правого выступа, в котором размещается считывающая головка скиммера. Таким образом, магнитная полоса карты считывается до того, как карточка втягивается банкоматом. Они могут считывать информацию с банковской карты с помощью телефона, в котором забита информация о карте.

Шимминг – это относительно новый вид мошенничества, который является, по своей сути, еще более технически усовершенствованной разновидностью скимминга. Устройство, которое считывает информацию с карты клиента банка в банкомате, тоньше человеческого волоса. Его абсолютно не видно, что позво-

ляет мошенникам практически безнаказанно опустошать банковский «пластик» и при этом оставаться незамеченными. По данным представителей компании *Cisco*, в результате данного вида мошенничества клиенты банков ежегодно теряют миллионы долларов. При вводе данных шиммер начинает свою работу и считывает все данные карты. Тонкая и гибкая прокладка при этом не мешает введению пластиковых карт. Шиммингговое устройство заметить просто невозможно. Но надо иметь в виду, что для мошенника только копирования информации с магнитной полосы недостаточно – ему нужно подсмотреть ПИН-код. Делается это с помощью миниатюрных камер или с помощью накладки на клавиатуру. Встречаются и более экзотические методы узнавания ПИН-кода, но в любом случае следование рекомендациям защиты от скимминга помогут спастись и от шимминга. Например, прикрытие свободной рукой клавиатуры при введении ПИН-кода не даст возможности шпионским мини-видеокамерам его зафиксировать.

При посещении гражданами банкомата внимательно осмотрите его лицевую сторону на предмет наличия накладок на клавиатуру, на картоприемник и других подозрительных приспособлений. Набирая ПИН-код, прикрывайте клавиатуру свободной рукой – так вы защитите свою финансовую информацию в том случае, если банкомат находится под наблюдением видеокамер мошенников. Старайтесь снимать деньги в банкоматах, расположенных в отделениях банков или в хорошо защищенных офисах. Как правило, скиммеры выбирают для своего промысла уличные терминалы. Также лучше воздержаться от оплаты картой на незнакомых заправках, в подозрительных кафе и магазинах.

Новым видом взлома банков с помощью устройств, схожих с функциональным устройством скимминга, является *BlackBox*. Данные атаки производятся методом подключения несанкционированного устройства к банкомату, что позволяет отправлять на него команды о выдаче денежных средств. Для того чтобы физически подключить такое устройство, мошенникам необходимо получить доступ к верхнему кабинету банкомата. Открытие верхней части банкомата происходит при помощи сверления или плавления отверстий.

Можно сказать, что на сегодняшний день *BlackBox* является «развивающимся трендом» среди существующих видов атак. Чтобы обезопасить банкомат, необходимо особое внимание уделить физической стороне защиты банкомата.

Для предотвращения данных преступлений, а также их для их расследования можно предложить следующий ряд действий:

1. Предоставить МВД России средства на улучшение материальной базы структур Министерства, занимающихся противодействием организованной преступности, совершенствование форм обмена информацией о преступлениях и преступниках [4–5], связанных с иностранными спецслужбами.

2. Повысить профессиональный уровень сотрудников соответствующих силовых структур, привлечь специалистов и общественность к правоохранительной деятельности.

3. Организовать фундаментальные и прикладные научные исследования в области обеспечения информационной безопасности Российской Федерации, разработать специальные методики, позволяющие выявлять и привлекать к от-

ветственности членов организованных преступных групп, занимающихся преступной деятельностью в сфере компьютерной информации.

4. Проведение профилактических бесед с сотрудниками и гражданами.

В современном обществе преступления с использованием скиммингового оборудования уменьшились вдвое. Эксперты Центрального банка Российской Федерации объясняют это тем, что появились банковские карты с чипами, которые защищают от мошенников-скиммеров. Также банки пытаются устанавливать антискимминговую защиту. Преступники же развивают скимминговое оборудование, поскольку это является наиболее быстрым и простым способом для снятия денежных средств у граждан, поэтому, несмотря на достижения банков, скимминг все еще является угрозой для современного общества.

Список литературы

1. Нагорный В. А. Скимминг в системе преступлений, сопряженных с использованием платежных карт: современное состояние, тенденции и проблемы уголовно-правовой квалификации // Методология и практика современной юриспруденции : сборник научных трудов. – 2014. – С. 87.

2. Сухаренко А. И. Скимминг вне закона // ЮРИСТ. – 2015. – № 37. – С. 3–5. – 2013. – С. 88.

3. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 134–135.

4. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. – 2019. – № 1. – С. 18-20.

5. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / Котляров И. И., Пузырева Ю. В. // Вестник экономической безопасности. – 2015. – № 7. – С. 60–61.

Яковлева Кристина Юрьевна[1]**,**
командир отделения 365 учебного взвода института подготовки сотрудников для органов предварительного расследования Московского университета МВД России имени В.Я. Кикотя

Андреев Алексей Владимирович[2]**,**
старший преподаватель кафедры уголовного процесса, кандидат юридических наук

КРИПТОВАЛЮТА КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 185.2 УК РФ

В настоящее время криптовалюта является очень важным и принципиально новым витком развития инвестиционных и транзакционных отношений, возникшим на основе сетевых технологий и ее финансовых особенностей. Все больше растет популярность биткоина как суррогата валюты. Тем не менее рост популярности биткоина и его популяризация во многих странах демонстрируют серьезные проблемы отсутствия регулирования, в том числе не только в торгово-биржевой деятельности, но и с точки зрения уголовного законодательства.

На сегодняшний день между экспертами во всем мире идут острые дискуссии относительно того, является ли допустимым легализировать биткоин как альтернативную цифровую денежную систему, нужно ли редактировать и издавать новые законы, регулирующие принципиально новый вид экономической деятельности, или необходимо запретить биткоин в принципе. Одной из наиболее популярных особенностей многих видов цифровой валюты является анонимность платежа, из-за чего происходит рост мошенничества, сетевых атак и спонсирования преступных группировок. Все это демонстрирует, что в уголовном законодательстве по причине отсутствия регулирования цифровой валюты в целом существует множество пробелов, которые связаны уже с махинациями вокруг цифровой валюты [1].

Также открытым остается вопрос, есть ли необходимость расширять нормы в Уголовном кодексе и Уголовно-процессуальном кодексе, включая квалифицирующие статьи за мошенничество и другие экономические преступления с цифровой валютой, либо создавать новые статьи, которые будут учитывать специфику цифровой валюты как принципиально нового предмета преступления и экономического института. Одна из проблем состоит также и в том, что на сегодняшний день за махинации с цифровой валютой теоретически невозможно привлечь к ответственности, потому что с точки зрения Уголовного кодекса Российской Федерации не существует такого предмета преступления, равно как и правовых понятий: цифровая валюта, криптовалюта [2]. Ранее Министерство финансов Российской Федерации готовило законопроект к Уголовному кодексу, добавляющий статью, которая посвящалась исключительно правовому регулированию преступлений, связанных с использованием криптовалюты, однако многими экспертами проект был раскритикован из-за неоправданно строгой

санкции сравнительно с остальными преступлениями в сфере экономической деятельности, и санкция была приближена к санкциям тяжких и особо тяжких преступлений против жизни и здоровья человека.

Очень важным на сегодняшний день является определение статуса криптовалюты в юридической практике в целом, является ли она деньгами, платежным инструментом, товаром или денежным суррогатом, и, в зависимости от определения статуса криптовалюты, в России есть необходимость сформировать закон или изменить существующее законодательство, чтобы затем можно было более основательно говорить про криптовалюту как предмет преступления [3]. Только после определения официального статуса криптовалюты можно устанавливать ответственность за ее незаконный учет или оборот. Также определение статуса криптовалюты сможет разделить с точки зрения закона легальный бизнес от черного (наркоторговли, продажи оружия и т. д.) Для ведения учета и мониторинга криптовалюты многие предлагают полностью ликвидировать принцип анонимности и сделать полностью прозрачные операции, введя для этого определенные параметры легитимности:

1. Сбор данных о клиенте.
2. Верификация документов.
3. Обозначение цели деловых отношений.
4. Определение бенефициарного собственника.
5. Мониторинг в соответствии с профилем риска. Прежде всего, необходимо определить параметры легитимности криптовалют [4–5].

В ст. 2 проекта федерального закона «О цифровых финансовых активах» впервые дается определение понятия «криптовалюта»: это вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций. Если исходить из концепции понимания криптовалют как финансовых инвестиционных активов, то их правовое положение близко к бездокументарным ценным бумагам, владение и распоряжение которыми осуществляется с помощью внесения изменений в цифровой реестр. В соответствии с действующим законодательством о ценных бумагах, бездокументарные ценные бумаги признаются объектами права собственности. Поэтому же пути идет и судебная практика [6]. Наличие прав у владельца бумаги фиксируется в специальном реестре с помощью средств электронно-вычислительной техники.

По этим признакам криптовалюты приближаются к признакам предмета преступления, указанном в ст. 185.2 УК РФ «Нарушение порядка учета прав на ценные бумаги» – права на ценные бумаги. Однако статус криптовалют как бездокументарных ценных бумаг не определен. Таким образом, этот законопроект дает основания для дальнейшего реформирования уголовного законодательства, в том числе для расширения предмета ст. 185.2 УК РФ. Полагаю, что необходимо установить уголовное наказание за нарушение правил ведения реестра цифровых транзакций при использовании криптовалюты.

Список литературы

1. Сидоренко Э. Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации // Библиотека криминалиста. – 2016. – № 3. – С. 36–40.

2. Сидоренко Э. Л. Антикоррупционные стандарты ОЭСР и их реализация в национальном уголовном праве (опыт прохождения странами третьей фазы оценки) // Журнал зарубежного законодательства и сравнительного правоведения. – 2014. – № 1. – С. 55–61.

3. Сидоренко Э. Л. Криптовалюта как новый юридический феномен // Информационая безопасность. – Москва. 2016. – № 3 (57). – С. 193–197.

4. Слушания Комитета по экономическим и монетарным вопросам Европарламента 25 января [Электронный ресурс] // URL: http://www.coindesk.com/europolno-evidence-linkingislamic-state-to-bitcoin (дата обращения: 15.10.2019).

5. О цифровых финансовых активах: проект федерального закона Министерства финансов Российской Федерации от 25 января 2018 г. [Электронный ресурс] // URL: https://www.minfin.ru/ru/document/?id_4=121810 (дата обращения: 15.10.2019).

6. Городецкая Я. С. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Я. С. Городецкая, В. В. Гончар, Д. Н. Захаров // Информационные технологии в правоохранительной деятельности: Сборник научных трудов XV научно-практической конференции. – 2017. – С. 91–96.

Иванова Анастасия Вячеславовна[1]**,**
студент Национального исследовательского технологического университета «МИСиС», группа БПИ17-1

Путилов Артур Олегович[2]**,**
старший преподаватель кафедры информатики и математики Московского университета МВД России имени В.Я. Кикотя

3D-МОДЕЛИРОВАНИЕ МЕСТА ПРЕСТУПЛЕНИЯ

Каждое место преступления похоже на образец ДНК – уникальное и не похожее на все остальные. Проблемы документирования этих мест преступления для правоохранительных органов остаются схожими для большинства случаев:

- ограничение по времени (особенно для аварийных сцен);
- возможное разрушение сцены и ее доказательств;
- пропущенные доказательства при первичном просмотре;
- физический объем документируемого места преступления при стандартном осмотре.

Этот последний пункт особенно сложен, поэтому выбор наиболее эффективного инструмента документирования сцены крайне важен. Рулетки и фотоаппараты были когда-то популярными и надежными способами документировать место преступления. Их эффективность, однако, в значительной степени зависела от интуиции следователя относительно того, какие доказательства было важно собрать.

Со временем были разработаны решения для смягчения этих проблем. 3D-сканирование является одним из таких решений, которое применяется правоохранительными органами.

Специалисту, использующему лазерный сканер, не нужно определять, какие доказательства собирать, поскольку сканер захватывает всю сцену. Одним из наиболее заметных преимуществ этой технологии является то, как мало времени требуется для сканирования сцены и ее полного документирования. Всего в нескольких настройках сканера в разных локациях сцены сканер может захватывать миллионы точек данных доказательства, которые образуют фотографическое облако точек.

Лазерный сканер является лишь одним из компонентов документации 3D-сцены. Другим важным компонентом является программное обеспечение, которое преобразует облако точек данных сцены в полезную трехмерную диаграмму или модель.

За рубежом полицейскими при осмотре места преступления используются следующие виды сканеров:

Лазерный сканер *FARO Focus* специально разработан для наружных применений, таких как аварии и места преступления, благодаря его небольшому размеру, небольшому весу и большой дальности – до 350 м, расширенным возможностям сканирования – даже под прямыми солнечными лучами – и про-

стоты позиционирования с помощью встроенного GPS-приемника. Удаленное сканирование с помощью лазерного сканера *Focus* и практически безграничный обмен данными сканирования делают это решение удобным и мобильным.

Другой сканер, *Leica Geosystems ScanStation PS40*, позиционирует себя как сканирующая станция. Данное устройство позволяет захватить очень большое пространство с большой точностью и небольшим временем на сканирование. Сканер *Leica* значительно упрощает процесс документирования места преступления и имеет большое преимущество, так как способен сканировать в любую погоду.

Для получения полной картины, особенно в случае ДТП, неоценимую помощь может оказать сканер, получающий 360-градусную панораму. Фактически и визуально передать то, что произошло на месте преступления или аварии, принципиально необходимо, и для этого существуют необходимые технологии. Это решение включает в себя камеру и штатив для съемки панорамных фотографий на 360 градусов, а также планшет для просмотра фотографий в реальном времени, чехол и программное обеспечение *OSCR*. Самая инновационная функция *OSCR360* – возможность виртуально представить место преступления или катастрофы, используя фотографии с 360-градусным размещением.

OSCR360 имеет аналого-цифровой преобразователь [1], а также является контейнером для мультимедийных файлов, которые потом могут быть использованы в качестве доказательств. Мультимедийные файлы, в том числе снятые на камеру кадры с камеры, видеорегистратор или видео с мобильного телефона, аудиозаписи, а также фотографии с крупным планом доказательств могут быть помещены в память *OSCR360*. Речевые сообщения как мультимедийные файлы также могут сохраняться в памяти устройства, причем частота дискретизации аудиофайлов позволяет их использовать для фоноскопической экспертизы [2].

В заключение можно отметить, что при использовании технологий моделирования и сохранения места совершения преступлений следователи всегда могут получить более полное и точное представление о совершенном преступлении, что в конечном итоге предоставит более точные доказательства в суде и поможет процессу расследования.

Список литературы

1. Жигалов К. Ю. Преодоление низкой частоты дискретизации аналого-цифрового преобразователя для задач синтеза речевого сигнала / К. Ю. Жигалов, В. Ю. Иванов // Прикладные исследования и технологии ART2015: сборник трудов Второй международной конференции. – 2015. – С. 148–150.

2. Иванов В. Ю., Маркова С. В. Моделирование истинных значений локальных максимумов амплитудного спектра в системах обработки речевой информации / В. Ю. Иванов, С. В. Маркова // Fractal Simulation. – 2014. – № 1 (6). – С. 27–29.

Абдрахманова Лидия Ринатовна[1]***,***
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Иванова Анастасия Вячеславовна[2]***,***
студент Национального исследовательского технологического университета
«МИСиС», группа БПИ17-1

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ «ОБЛАЧНЫХ» ХРАНИЛИЩ

На сегодняшний день практически в каждом доме есть персональный компьютер. Все это появилось не так давно, но стало неотъемлемой частью нашей жизни. На персональном компьютере пользователи хранят файлы, которые необходимы для учебы, работы и личного пользования. Никто не готов потерять все свои документы из-за поломки техники.

Также существует еще одна проблема, с которой сталкиваются многие пользователи, – необходимость в удобной передаче файлов между компьютерами. Привычные для нас способы, такие как флеш-накопители, жесткие диски, имеют свои недостатки. Например: нехватка свободного места на носителе. Чтобы решить данный вопрос и сделать доступность файлов немного проще, создали облачные хранилища.

Существуют интернет-сервисы, которые предоставляют возможность хранить файлы на них. По факту, мы загружаем их на какой-то удаленный компьютер в сети Интернет, на котором они хранятся, доступ к которым мы можем получить по адресу сервиса, который предоставил такую возможность. Эта технология позволяет не думать пользователю о способе размещения своей информации. Он имеет выделенный ему объем свободного места и может использовать его по своему усмотрению. В российском интернете наиболее известны такие облачные хранилища, как «Яндекс.Диск», «Облако@mail.ru», *Google Drive, Dropbox, iCloud, OneDrive*. Практически все облачные хранилища имеют как бесплатное, так и платное аккаунты. В разных сервисах доступен разный объем памяти в бесплатном варианте. При необходимости можно докупить место на сервере, где объем и цена будут зависеть от конкретного облачного хранилища.

Преимущества облачных хранилищ

Во-первых, облачные хранилища очень удобны для передачи файлов больших размеров, так как по электронной почте размеры файлов ограничены несколькими сотнями мегабайт. Например, если вы хотите поделиться своими фотографиями с отпуска со своими знакомыми, то подборку из пары сотен фотографий лучше загрузить в облачное хранилище, а вашим знакомым – переслать ссылку в электронном письме.

Во-вторых, можно получить доступ к информации через сеть Интернет с любого компьютера и из любой точки мира. Если вы работаете над документами совместно с вашими коллегами, то размещение документов в одном облачном хранилище даст доступ к одному и тому же документу, благодаря чему пропадет необходимость постоянной пересылки документа от одного человека к другому и не будет появляться множества копий документа. Также можно установить определенные программы, которые устанавливаются на любое устройство, благодаря которым будет возможен постоянный доступ к файлам, загруженным в облако.

Третье преимущество облачных сервисов: они используют технологии резервирования данных, т. е. для всех данных, которые загружаются в облако, используется резервное хранение. Это уменьшает вероятность потери данных даже в случае аппаратного сбоя, как у конечного пользователя, так и у провайдера облачного хранилища. Речь идет о накопителе на магнитном диске компьютера пользователя, если данные хранились на нем, так и о потере данных непосредственно на облачном сервисе, так как данные тоже хранятся на различных накопителях компьютеров, которые относятся к структуре сервисов облачных хранилищ.

Недостатки облачных хранилищ

Остается открытым вопрос безопасности. Не стоит забывать, что ко всем загруженным файлам имеет доступ сам сервер и его сотрудники. Очень многое зависит от того, каким образом происходит хранение файлов на самом сервере, тем не менее физически к информации имеет доступ сам сервер. Если произойдет какая-либо хакерская атака, и случится взлом серверов облачного хранилища, то все загруженные файлы могут попасть в открытый доступ.

Главными угрозами безопасности в «облаке» являются:

1. Кража данных.

Кража конфиденциальной информации всегда пугает организации, так как, по их мнению, «облако» открывает новые пути атак для злоумышленников. При недостаточном продумывании архитектуры облачного сервиса изъян в приложении одного из клиентов может открыть злоумышленникам доступ к данным ко всем пользователям сервиса.

У каждого «облака» есть несколько уровней защиты, каждый из которых защищает информацию на своем уровне.

Первый уровень защиты – это физическая защита сервера. Речь идет о воровстве или порче носителей информации. Для обеспечения безопасности своих серверов организации хранят информацию в дата-центрах с видеонаблюдением, охраной и ограничением доступа не только от посторонних, но и от большинства сотрудников компании. Так что вероятность того, что злоумышленник пройдет и заберет информацию, близка нулю.

Многие SaaS-компании[1] не держат всю информацию на одном сервере, а распределяют ее, иногда даже территориально. Таким образом, взлом не при-

[1] *SaaS* (*software as a service*) – одна из форм облачных вычислений, модель обслуживания, при которой пользователям предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером.

несет ущерба, угрожающего пользователю. Как показывает практика, чаще всего при взломе сервера воруют базу адресов электронной почты. Это значит, что пользователь получит спам-сообщения на свой почтовый ящик.

Второй уровень защиты – защита в процессе передачи данных.

SaaS-компании шифруют весь трафик с помощью https-протокола с использованием SSL-сертификата. Так данные будут в безопасности от попыток анализаторов траффика перехватить их. *Http* (*Hypertext Transfer Protocol*) – базовый протокол передачи данных между клиентом и сервером. По этому протоколу данные между браузером и клиентом отсылаются в виде обычного текста, позволяя владельцу сети видеть содержимое. Это проблема безопасности, поэтому был разработан протокол *HTTP Secure* (*HTTPS*), позволяющий пользователю и серверу сначала установить зашифрованное соединение, а после отправлять http-сообщения, не волнуясь, что их прочитают третьи лица. SSL-сертификат – это цифровая подпись сайта, которая необходима для безопасного соединения. При его помощи вся информация между пользователем и сайтом шифруется таким образом, что она становится нечитаемой для других лиц (мошенников, системных администраторов и провайдеров). Также он является подтверждением подлинности сайта.

2. Потеря данных.

Потеря данных в облачном хранилище может произойти не только по вине злоумышленников, но и по другой причине. Данные случайно может удалить сам провайдер, или они пострадают при стихийном бедствии или пожаре. Однако такое может произойти крайне редко. Компании постоянно и не менее двух раз в сутки автоматически копируют всю информацию. Таким образом, в случае потери данных пользователь всегда может обратиться в техническую поддержку, и информацию можно будет восстановить.

3. Кража аккаунтов.

В облачной среде взломщик может использовать украденную регистрационную информацию, чтобы перехватывать, подделывать или выдавать искаженные данные реальных пользователей. Впоследствии это можно использовать для перенаправления их на вредоносные сайты. Данные действия можно обнаружить в процессе исследования компьютерного инцидента, однако сам пользователь может нанести себе и своим знакомым существенный вред [1]. Внедрение надежной двухфакторной аутентификации позволит снизить этот риск. Также уменьшает риск запрет использования одних и тех же паролей для всех сервисов.

4. Незащищенные интерфейсы и *API*

Слабые интерфейсы ПО, или *Application Programming Interface* (*API*), используемые заказчиками для управления и взаимодействия с облачными услугами, подвергают пользователей целому ряду угроз, особенно если они размещены в социальных сетях [2]. Эти интерфейсы должны быть правильно спроектированы и обязательно включать аутентификацию, управление доступом и шифрование, чтобы обеспечить необходимую защиту и готовность облачных услуг.

Организации и сторонние подрядчики часто используют облачные интерфейсы для предоставления дополнительных услуг, что делает их более сложными и увеличивает риск, поскольку может потребоваться, чтобы заказчик сообщил свои регистрационные данные такому подрядчику для упрощения предоставления услуг.

5. DDoS-атаки

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объем системных ресурсов и не давая заказчикам пользоваться этой услугой.

6. Злонамеренный инсайдер

В среде *IaaS, PaaS* или *SaaS,* в которой не обеспечен должный уровень безопасности, инсайдер, имеющий корыстные намерения (например, системный администратор), может получить доступ к конфиденциальной информации, которая ему не предназначена.

Используемая литература

1. Попов Д. О. Правовые основы проведения компьютерной технической экспертизы / Д. О. Попов, В. Ю. Иванов // Технологии информационной безопасности в деятельности органов внутренних дел: X–XI научно-практическая конференция. – 2014. – С. 116–122.

2. Родкина Е. А., Иванов В. Ю. Некоторые аспекты мониторинга социальных сетей / Е. А. Родкина, В. Ю. Иванов // Технологии информационной безопасности в деятельности органов внутренних дел: Сборник научных трудов XIII научно-практической конференции. – 2016. – С. 86–89.

Еськов Александр Васильевич[1],
профессор кафедры информационной безопасности
Краснодарского университета МВД России,
доктор технических наук, профессор

Дзасохова Виктория Вячеславовна[2],
курсант Краснодарского университета МВД России

РИСКИ И ЗАДАЧИ, СВЯЗАННЫЕ С АНТИТЕРРОРИСТИЧЕСКИМ ПРОТИВОДЕЙСТВИЕМ В СЕТИ ИНТЕРНЕТ

Одним из главных рисков противодействия пропаганды терроризма в сетевом пространстве называют неэффективную работу органов власти и силовых ведомств по формированию антитеррористического мышления пользователей. В основном государственные органы и министерства предпринимают действия, направленные на обнаружение и раскрытие террористических сайтов, а также создание доказательственной базы в отношении их незаконных действий.

Нужно отметить, что благодаря созданию портала «Наука и образование против террора» (*scienceport.ru*) Министерством науки и высшего образования стало возможно создание системы совместной работы отдельных вузов по наполнению страниц и сайтов антитеррористической информацией.

Однако в условиях современности появилась необходимость повысить активность индивидуальной работы с пользователями сети, выражающих интерес к тематике терроризма и экстремизма. Нормативно-правовая база Российской Федерации позволяет осуществлять работу по ограничению доступа к экстремистским и террористическим интернет-ресурсам несколькими путями. К ним относятся:

– блокировка сетевых адресов; прекращение работы домена, при расположении его интернет ресурса в доменнзонах «ru» и «рф»;

– фильтрация трафика на пограничных маршрутизаторах интернет-провайдеров.

При этом появляются различные проблемы, как правового типа, так и организационного.

Одна из основных проблем – это отсутствие международных соглашений, контролирующих работу этих сайтов и блокирующих доступ к ним. В данное время этот вопрос так и не имеет решения. Это связано не только с тем, что во всех странах по-разному толкуют понятия, связанные с экстремисткой и террористической деятельностью, но с явным нежеланием зарубежных партнеров вести такие переговоры.

Следующая проблема заключается в подготовке нашего государства в участии такого рода переговорах. Еще одна юридическая проблема заключается в недостатках законодательного регулирования правового статуса и ответственности лиц, осуществляющих деятельность в сети и дающих право доступа к сети

Интернет пользователям. Привлечь их к уголовной ответственности практически невозможно. Технически регистрация доменных имен сайтов происходит в одной стране, а работа осуществляется в другой. Это образует дополнительные сложности при их обнаружении. О пунктах коллективного пользования, где возможно установить личность пользователя сети невозможно, речь уже шла ранее.

Следующая группа рисков связана с анализом экстремистских и террористических материалов. Отсутствуют квалифицированные специалисты, не регламентированы и не унифицированы методы отнесения к запрещенным материалам, да и сама совместная работа специалистов, следователей и судей. Формирование Федерального списка экстремистских материалов ведется не системно. Часто можно наблюдать случаи, когда по одним и тем же интернет-ресурсам выносятся несколько судебных решений или одни электронные копии с другими реквизитами не признаются экстремистскими. Обособленный блок проблем – внедрение в практическую деятельность результатов научных исследований и образовательных данных.

В современное время имеется значительный научно-методический материал по теме контрпропаганды, хотя его внедрение в жизнь во многих случаях заключается в рассылке по учебным заведениям и представлении на конференциях. При этом отсутствует проверка их применения в реальной практике учебной деятельности. Одной из задач, устанавливаемых перед информационно-аналитическим порталом *scienceport.ru,* как раз и становится преобразование его в методологическую и методическую площадку, на которой можно не только разместить различные антиэкстремистские и антитеррористические данные, но и осуществить их интеграцию в деятельность учебного и научных процессов.

Успешное формирование антитеррористического сознания у неопытных пользователей сети Интернет в первую очередь зависит от существования достаточной материальной и ресурсной поддержки; разработки и проведения действенной молодежной политики, выполнения антикоррупционных программ, размеренной государственной политики в сфере культуры религии и образования. Хотя и главной остается проблема – кем это будет реализовываться?

Лицо, которое управляет антитеррористическим порталом, общается с пользователями и должно иметь психологические, педагогические навыки, иметь навыки журналиста, умело владеть компьютерными технологиями. Кроме того, иметь доступ к различным интернет-ресурсам, владеть хотя бы одним иностранным языком; хорошо разбираться в этнических, религиозных и культурных обычаях страны и региона, и при этом делать это не на общественных началах. В настоящее время, к сожалению, подготовка таких специалистов в структуре высшего образования проходит слабо, несмотря на то, что некоторые компетенции подготовки, указанные в различных нормативных актах, прямо или косвенно дают возможность это делать. Здесь следует отметить, что в данной сфере необходимо улучшать подготовку магистров и систему повышения квалификации на постоянной основе. Безусловно, одному человеку, даже специалисту по пропаганде контртерроризма в сети Интернет, сложно все это делать. Для продуктивной деятельности необходимо иметь группу специалистов различных направлений. Кроме того, эти сотрудники должны не только понимать методы

идеологического воздействия, которыми пользуются террористические организации в интернет-пространстве, но и уметь применять современные способы социальной инженерии, когда общение происходит в Сети, когда настоящая личность человека остается неизвестной.

Список литературы

1. Методические рекомендации по выявлению признаков подготовки совершения террористических актов [Электронное издание] / С. Е. Васюков // URL: http://scienceport.ru/library/methodical/metodicheskie-rekomendatsii-povyyavleniyu-priznakov-podgotovki-soversheniya-terroristicheskikh-aktov.

2. Основы противодействия экстремизму и терроризму : учебное пособие / Чувашский государственный университет имени И.Н. Ульянова // URL: http://scienceport.ru/library/-literature/osnovyprotivodeystviya-ekstremizmu-i-terrorizmu.

3. Профилактика экстремизма и террористического поведения молодежи в интернет-пространстве: традиционные и инновационные формы : методические рекомендации [Электронное издание]. – Р/н-Д : М. : Кредо, 2018. // URL: https://minobrnauki.gov.ru/common/upload/library/antiterror/metodichka_soderzhanie_03.12.2018-1.pdf.

Сборник научных трудов Всероссийской конференции
«Борьба с киберпреступностью в условиях развития цифрового общества»

Борьба с киберпреступностью в условиях развития цифрового общества

Научное электронное издание

Корректор *Чеботарева С. О.*
Компьютерная верстка *Фомин И. Е.*
11,52 усл. печ. л.

Систем. требования: CPU 1,5 Гц; RAM 512 Мб; Windows XP SP3;
1 Гб свободного места на жестком диске.
Подписано к изданию 26.12.2019 г.

ISBN 978-5-9694-0824-1

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12